

Cisco IOS IP Routing: BGP Command Reference

November 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco IOS IP Routing: BGP Command Reference
© 2010 Cisco Systems, Inc. All rights reserved.



CONTENTS

Introduction IRG-1

BGP Commands IRG-3

address-family ipv4 (BGP) IRG-4
address-family l2vpn IRG-8
address-family nsap IRG-10
address-family rtfilter unicast IRG-12
address-family vpnv4 IRG-14
aggregate-address IRG-16
auto-summary (BGP) IRG-19
bgp additional-paths install IRG-22
bgp advertise-best-external IRG-23
bgp aggregate-timer IRG-25
bgp always-compare-med IRG-27
bgp asnotation dot IRG-29
bgp bestpath as-path ignore IRG-33
bgp bestpath compare-routerid IRG-34
bgp bestpath cost-community ignore IRG-35
bgp bestpath med confed IRG-37
bgp bestpath med missing-as-worst IRG-39
bgp client-to-client reflection IRG-40
bgp cluster-id IRG-42
bgp confederation identifier IRG-44
bgp confederation peers IRG-47
bgp dampening IRG-50
bgp default ipv4-unicast IRG-52
bgp default local-preference IRG-53
bgp deterministic-med IRG-54
bgp dmzlink-bw IRG-57
bgp enforce-first-as IRG-59
bgp fast-external-fallover IRG-60

bgp graceful-restart **IRG-62**
bgp inject-map **IRG-65**
bgp listen **IRG-67**
bgp log-neighbor-changes **IRG-69**
bgp maxas-limit **IRG-71**
bgp nexthop trigger delay **IRG-73**
bgp nexthop trigger enable **IRG-74**
bgp nexthop **IRG-75**
bgp nopeerup-delay **IRG-78**
bgp recursion host **IRG-80**
bgp redistribute-internal **IRG-85**
bgp regexp deterministic **IRG-87**
bgp router-id **IRG-89**
bgp rr-group **IRG-91**
bgp scan-time **IRG-93**
bgp slow-peer detection **IRG-95**
bgp slow-peer split-update-group dynamic **IRG-97**
bgp soft-reconfig-backup **IRG-99**
bgp suppress-inactive **IRG-101**
bgp transport **IRG-103**
bgp update-delay **IRG-104**
bgp update-group split as-override **IRG-106**
bgp upgrade-cli **IRG-108**
bgp-policy **IRG-110**
clear bgp nsap **IRG-113**
clear bgp nsap dampening **IRG-115**
clear bgp nsap external **IRG-116**
clear bgp nsap flap-statistics **IRG-117**
clear bgp nsap peer-group **IRG-118**
clear ip bgp **IRG-119**
clear ip bgp dampening **IRG-123**
clear ip bgp external **IRG-125**
clear ip bgp flap-statistics **IRG-128**
clear ip bgp in prefix-filter **IRG-130**
clear ip bgp ipv4 **IRG-131**

clear ip bgp ipv6 **IRG-135**
clear ip bgp l2vpn **IRG-139**
clear ip bgp peer-group **IRG-142**
clear ip bgp table-map **IRG-145**
clear ip bgp update-group **IRG-147**
clear ip bgp vpnv4 **IRG-149**
clear ip bgp vpnv4 unicast dampening **IRG-153**
clear ip bgp vpnv6 **IRG-155**
clear ip bgp vpnv6 unicast dampening **IRG-159**
clear ip prefix-list **IRG-161**
continue **IRG-162**
default-information originate (BGP) **IRG-166**
default-metric (BGP) **IRG-168**
distance bgp **IRG-170**
distribute-list in (BGP) **IRG-172**
distribute-list out (BGP) **IRG-174**
exit-peer-policy **IRG-176**
exit-peer-session **IRG-177**
export map **IRG-178**
ha-mode graceful-restart **IRG-180**
import ipv4 **IRG-182**
import path limit **IRG-184**
import path selection **IRG-186**
inherit peer-policy **IRG-188**
inherit peer-session **IRG-190**
ip as-path access-list **IRG-192**
ip bgp fast-external-fallover **IRG-195**
ip bgp-community new-format **IRG-196**
ip community-list **IRG-198**
ip extcommunity-list **IRG-202**
ip policy-list **IRG-208**
ip prefix-list **IRG-210**
ip prefix-list description **IRG-213**
ip prefix-list sequence-number **IRG-215**
ip verify unicast vrf **IRG-216**

match as-path IRG-218
match community IRG-220
match extcommunity IRG-222
match local-preference IRG-224
match policy-list IRG-226
match source-protocol IRG-228
maximum-paths eibgp IRG-231
maximum-paths ibgp IRG-234
neighbor activate IRG-238
neighbor advertise-map IRG-241
neighbor advertisement-interval IRG-243
neighbor capability orf prefix-list IRG-245
neighbor default-originate IRG-247
neighbor description IRG-249
neighbor disable-connected-check IRG-251
neighbor distribute-list IRG-253
neighbor dmzlink-bw IRG-256
neighbor ebgp-multihop IRG-258
neighbor fall-over IRG-260
neighbor filter-list IRG-263
neighbor ha-mode graceful-restart IRG-265
neighbor ha-mode sso IRG-267
neighbor inherit peer-policy IRG-268
neighbor inherit peer-session IRG-270
neighbor local-as IRG-272
neighbor maximum-prefix IRG-277
neighbor maximum-prefix (BGP) IRG-279
neighbor next-hop-self IRG-282
neighbor next-hop-unchanged IRG-284
neighbor password IRG-286
neighbor peer-group (assigning members) IRG-289
neighbor peer-group (creating) IRG-291
neighbor prefix-list IRG-294
neighbor remote-as IRG-297
neighbor remove-private-as IRG-303

neighbor route-map **IRG-306**
neighbor route-reflector-client **IRG-308**
neighbor send-community **IRG-310**
neighbor shutdown **IRG-312**
neighbor slow-peer detection **IRG-314**
neighbor slow-peer split-update-group dynamic **IRG-317**
neighbor slow-peer split-update-group static **IRG-319**
neighbor soft-reconfiguration **IRG-320**
neighbor soo **IRG-322**
neighbor timers **IRG-325**
neighbor transport **IRG-327**
neighbor ttl-security **IRG-330**
neighbor unsuppress-map **IRG-332**
neighbor update-source **IRG-334**
neighbor version **IRG-336**
neighbor weight **IRG-338**
network (BGP and multiprotocol BGP) **IRG-340**
network backdoor **IRG-342**
redistribute (BGP to ISO IS-IS) **IRG-344**
redistribute (IP) **IRG-347**
redistribute (ISO IS-IS to BGP) **IRG-354**
redistribute dvmrp **IRG-356**
router bgp **IRG-358**
scope **IRG-363**
set as-path **IRG-365**
set comm-list delete **IRG-368**
set community **IRG-370**
set dampening **IRG-372**
set extcommunity **IRG-374**
set extcommunity cost **IRG-378**
set ip next-hop (BGP) **IRG-381**
set metric (BGP-OSPF-RIP) **IRG-384**
set metric-type internal **IRG-386**
set origin (BGP) **IRG-388**
set traffic-index **IRG-390**

set weight **IRG-392**
show bgp all community **IRG-394**
show bgp all neighbors **IRG-397**
show bgp nsap **IRG-402**
show bgp nsap community **IRG-405**
show bgp nsap community-list **IRG-408**
show bgp nsap dampened-paths **IRG-410**
show bgp nsap dampening **IRG-412**
show bgp nsap filter-list **IRG-415**
show bgp nsap flap-statistics **IRG-417**
show bgp nsap inconsistent-as **IRG-420**
show bgp nsap neighbors **IRG-422**
show bgp nsap paths **IRG-429**
show bgp nsap quote-regexp **IRG-431**
show bgp nsap regexp **IRG-433**
show bgp nsap summary **IRG-435**
show ip as-path-access-list **IRG-438**
show ip bgp **IRG-440**
show ip bgp all dampening **IRG-449**
show ip bgp cidr-only **IRG-451**
show ip bgp community **IRG-453**
show ip bgp community-list **IRG-455**
show ip bgp dampened-paths **IRG-458**
show ip bgp dampening dampened-paths **IRG-460**
show ip bgp dampening flap-statistics **IRG-462**
show ip bgp dampening parameters **IRG-465**
show ip bgp filter-list **IRG-467**
show ip bgp flap-statistics **IRG-469**
show ip bgp inconsistent-as **IRG-471**
show ip bgp injected-paths **IRG-472**
show ip bgp ipv4 **IRG-474**
show ip bgp ipv4 multicast **IRG-476**
show ip bgp ipv4 multicast summary **IRG-478**
show ip bgp l2vpn **IRG-480**
show ip bgp neighbors **IRG-484**

show ip bgp paths **IRG-501**
show ip bgp peer-group **IRG-503**
show ip bgp quote-regexp **IRG-505**
show ip bgp regexp **IRG-509**
show ip bgp replication **IRG-512**
show ip bgp rib-failure **IRG-514**
show ip bgp rtfilter **IRG-516**
show ip bgp summary **IRG-518**
show ip bgp template peer-policy **IRG-524**
show ip bgp template peer-session **IRG-527**
show ip bgp update-group **IRG-529**
show ip bgp vpnv4 all sso summary **IRG-532**
show ip bgp vpnv4 **IRG-533**
show ip bgp vpnv4 all dampening **IRG-542**
show ip bgp vpnv6 unicast all dampening **IRG-544**
show ip community-list **IRG-546**
show ip extcommunity-list **IRG-548**
show ip policy-list **IRG-551**
show ip prefix-list **IRG-552**
show ip route **IRG-554**
show ip route vrf **IRG-567**
show tcp ha connections **IRG-573**
slow-peer detection **IRG-575**
slow-peer split-update-group dynamic **IRG-577**
slow-peer split-update-group static **IRG-579**
soo **IRG-580**
synchronization **IRG-583**
table-map **IRG-585**
template peer-policy **IRG-587**
template peer-session **IRG-590**
timers bgp **IRG-593**



Introduction

This book describes the commands used to configure and monitor Border Gateway Protocol (BGP) routing capabilities and features.

For BGP configuration information and examples, refer to the *Cisco IOS IP Routing: BGP Configuration Guide*.



BGP Commands

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** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]

no address-family ipv4 [**mdt** | **multicast** | **tunnel** | **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.
multicast	(Optional) Specifies IPv4 multicast address prefixes.
tunnel	(Optional) Specifies an IPv4 routing session for multipoint tunneling.
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 integrated into Cisco IOS Release 12.0(28)S, and the **tunnel** keyword was added.
12.0(29)S	The **mdt** keyword was added.
12.0(30)S	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	Support for the router scope configuration mode was added.

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 Routers.
12.4(20)T	The **mdt** keyword was added.

Usage Guidelines

The **address-family ipv4** command replaces the **match nlri** and **set nlri** commands. The **address-family ipv4** command places the router 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 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 a**ddress-family ipv4 multicast**, 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 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 Multi-Topology 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 router in address family configuration mode for the IPv4 address family:

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

Multicast Example

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

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

Unicast Example

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

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

VRF Example

The following example places the router 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:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 vrf cisco
Router(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.

Tunnel Example

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

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

MDT Example

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

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

Router Scope Configuration Mode Example

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 router enters router scope address family configuration mode, and only multicast address prefixes for the IPv4 address family are specified:

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

Related Commands

Command	Description
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.

Command	Description
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 [**vpls**]

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

Syntax Description

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 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.

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.



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 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

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 Automated Route Target Filtering with a BGP peer, use the **address-family rtfilter unicast** command in router configuration mode. To remove ARTF, 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 RT Constraint 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.

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 RT constraint (RTC) network layer reachability information (NLRI) to a route reflector (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
 exit-address-family
```

In the following example, the local PE is configured with the RT Constraint 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 10.2.2.2 default-originate
 exit-address-family
```

In the following example, the RR is configured with the RT Constraint 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 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 [**unicast**]

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

Syntax Description

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

Defaults

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 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

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.

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)#
```

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

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.
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.

Release	Modification
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.

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** command when 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.
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.

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
Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode support was added.
12.2(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 Table 1.

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 install

To enable 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.

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.
- 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
bgp advertise-best-external	Enables BGP to use an external route as the backup path after a link or node failure.

bgp advertise-best-external

To enable 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 2.5	This command was integrated into Cisco IOS XE Release 2.5.

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.
- 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
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

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.

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. Table 2 and Table 3 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 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

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

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 HistoryR

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.

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
Router configuration

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 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.

Defaults

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

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.

Defaults

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

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 client-to-client reflection

To enable or restore 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

no bgp client-to-client reflection

Syntax Description

This command has no arguments or keywords.

Defaults

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

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.

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** command to disable client-to-client reflection.

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, client-to-client reflection is disabled with the **no bgp client-to-client reflection** command.

```
Router(config)# router bgp 50000
Router(config-router)# neighbor 10.24.95.22 route-reflector-client
Router(config-router)# neighbor 10.24.95.23 route-reflector-client
Router(config-router)# neighbor 10.24.95.24 route-reflector-client
Router(config-router)# no bgp client-to-client reflection
Router(config-router)# 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.
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 cluster-id	Configures the cluster ID if the BGP cluster has more than one route reflector.
neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
show ip bgp	Displays entries in the BGP routing table.

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.

Defaults

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

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.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

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

Usage Guidelines

The **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.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

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

Usage Guidelines

The **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 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.

Defaults

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
Router configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	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.
12.2SX	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.
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

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.

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:

```
Router(config)# router bgp 50000
Router(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

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

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.

Usage Guidelines

The **bgp always-compare-med** command is used to enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. After the **bgp always-compare-med** command is configured, all paths for the same prefix that are received from different neighbors, which are in the same autonomous system, will be grouped together and sorted by the ascending MED value (received-only paths are ignored and not grouped or sorted). The best path selection algorithm will then pick the best paths using the existing rules; the comparison is made on a per neighbor autonomous system basis and then global basis. The grouping and sorting of paths occurs immediately after this command is entered. For correct results, all routers in the local autonomous system must have this command enabled (or disabled).

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

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.

Defaults

The behavior of this command is enabled by default.

Command Modes

Router configuration

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 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

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 [**restart-time** *seconds* | **stalepath-time** *seconds*] [**all**]

no bgp graceful-restart

Syntax Description

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 (router-config)

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.
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.

Release	Modification
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 .

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 soft or hard reset.

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

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
```

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 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
Router configuration

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 [**limit** *max-number* | **range** *network/length* **peer-group** *peer-group-name*]

no bgp listen [**limit** | **range** *network/length* **peer-group** *peer-group-name*]

Syntax Description

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.

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 intergrated 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.

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.

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

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.

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:

```
Router(config)# bgp router 40000
Router(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

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 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 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.

Command Modes

Address family configuration
Router configuration

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.
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.

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 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 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), Virtual Private Network (VPN) Version 4 (VPNv4), and Virtual Routing and Forwarding (VRF) 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.

Usage Guidelines

The **bgp recursion host** command is used to help Cisco Express Forwarding during traffic blackholing 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 are 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
```

Table 4 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.
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.

Table 4 show ip bgp vpnv4 vrf network-address Field Descriptions (continued)

Field	Description
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
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 return the router to default behavior and 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.

Defaults

IBGP routes are not redistributed into IGPs.

Command Modes

Address family configuration
Router configuration

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.

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 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 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

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

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 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 family configuration 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.

Defaults

No default behavior or values

Command Modes

VPNv4 address family configuration

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 of BGP routing information. • Valid values are from 15 to 60 seconds. The default is 60 seconds.

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 is increased from 5 seconds to 15 seconds.
15.0(1)S	This command was modified. The minimum scan time is increased from 5 seconds to 15 seconds.
Cisco IOS XE 3.1S	This command was modified. The minimum scan time is increased from 5 seconds to 15 seconds.

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.

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 vpn4 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
Router configuration

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.
show ip bgp neighbors	Displays information about the TCP and Border Gateway Protocol (BGP) connections to neighbors.

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
Router configuration

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.

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.

Examples

In the following example, the BGP routing process is configured to not advertise routes that are not installed in the RIB:

```
Router(config)# router bgp 500000
Router(config-router)# address-family ipv4
Router(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

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 VPNv4 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

VPNv4 address-family

Command History

Release	Modification
12.2(33)SRD4	This command was introduced.

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).



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

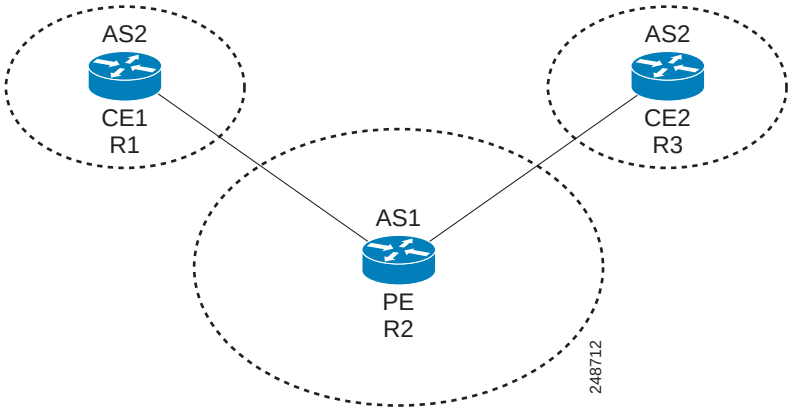
In the following example, the **neighbor as-override** command is configured on a PE for neighbors CE1 and CE2. When CE1 advertises a route to the PE, this command replaces the peer AS number (2) in the AS path with its own AS number (1) before advertising the route to its peers, in this case, CE2. Enabling 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 as 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. Figure 1 illustrates the PE in AS1 and the two CEs in AS2.

Figure 1 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

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 Table 1 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

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 source and 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-int)# bgp-policy source ip-prec-map
Router(config-int)# 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.

clear bgp nsap

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

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

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

- BGP timer specification change
- BGP administrative distance changes

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

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

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

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

Examples

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

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

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

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

Related Commands

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

clear bgp nsap dampening

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

clear bgp nsap dampening [*nsap-prefix*]

Syntax Description

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

Command Default

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

clear bgp nsap external

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

clear bgp nsap flap-statistics

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

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

Syntax Description

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

Command Default

No statistics are cleared.

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

clear bgp nsap peer-group

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

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

Syntax Description

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

Command Default

No BGP TCP connections are cleared.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

clear ip bgp

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

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

Usage Guidelines

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



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

Generating Updates from Stored Information

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

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

Use this command whenever any of the following changes occur:

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

Dynamic Inbound Soft Reset

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

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

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

Related Commands

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

clear ip bgp dampening

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

Syntax Without Address Family Syntax

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

Syntax With Address Family Syntax

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

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

Examples

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

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

Related Commands

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

clear ip bgp external

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

Syntax Without Address Family Syntax

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

Syntax With Address Family Syntax

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

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

Usage Guidelines

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

Generating Updates from Stored Information

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

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

Use this command whenever any of the following changes occur:

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

Dynamic Inbound Soft Reset

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

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

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

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

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

Examples

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

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

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

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

Related Commands

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

clear ip bgp flap-statistics

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

Syntax Without Address Family Syntax

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

Syntax With Address Family Syntax

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.0(22)S	The **vpnv4** and **ipv4** keywords were added.
12.0(29)S	The **mdt** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

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

Examples

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

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

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

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

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

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

Related Commands

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

clear ip bgp in prefix-filter

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

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

clear ip bgp ipv4

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The **mdt** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.4(20)T	This command was modified. The **mdt** keyword was added.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(2)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

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

Generating Updates from Stored Information

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

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

Use this command whenever any of the following changes occur:

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

Dynamic Inbound Soft Reset

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

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

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

Related Commands

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

clear ip bgp ipv6

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(2)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

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

Generating Updates from Stored Information

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

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

Use this command whenever any of the following changes occur:

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

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

Dynamic Inbound Soft Reset

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

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

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

Related Commands

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

clear ip bgp l2vpn

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

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

Syntax Description

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

Command Default

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

Command Modes

Privileged EXEC (#)

Command History

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

Release	Modification
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(2)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

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

Generating Updates from Stored Information

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

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

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

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

Dynamic Inbound Soft Reset

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

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

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

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

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

Examples

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

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

Related Commands

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

clear ip bgp peer-group

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

Syntax Without Address Family Syntax

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

Syntax With Address Family Syntax

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.0(2)S	This command was integrated into Cisco IOS Release 12.0(2)S, and dynamic inbound soft reset capability was added.
12.0(7)T	The dynamic inbound soft reset capability was integrated into Cisco IOS Release 12.0(7)T.
12.0(22)S	The **vpnv4** and **ipv4** keywords were added.
12.0(29)S	The **mdt** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

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

Generating Updates from Stored Information

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

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

Use this command whenever any of the following changes occur:

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

Dynamic Inbound Soft Reset

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

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

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

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

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

Examples

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

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

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

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

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

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

Related Commands

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

clear ip bgp table-map

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

Syntax Without Address Family Syntax

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

Syntax With Address Family Syntax

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.0(21)S	This command was integrated into Cisco IOS Release 12.0(21)S.
12.0(22)S	The **vpnv4** and **ipv4** keywords were added.
12.1(13)E	This command was integrated into Cisco IOS Release 12.1(13)E.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

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

Examples

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

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

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

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

Related Commands

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

clear ip bgp update-group

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

Syntax Without Address Family Syntax

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

Syntax With Address Family Syntax

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Release	Modification
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(29)S	The **mdt** keyword was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

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

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

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

Examples

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

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

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

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

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

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

Related Commands

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

clear ip bgp vpnv4

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(2)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

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

Generating Updates from Stored Information

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

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

Use this command whenever any of the following changes occur:

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

Dynamic Inbound Soft Reset

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

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

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

Related Commands

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

clear ip bgp vpnv4 unicast dampening

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

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

clear ip bgp vpnv6

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.

Release	Modification
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

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

Generating Updates from Stored Information

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

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

Use this command whenever any of the following changes occur:

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

Dynamic Inbound Soft Reset

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

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

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

Related Commands

Command	Description

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

clear ip bgp vpnv6 unicast dampening

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

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

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

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

clear ip prefix-list

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
distribute-list in (IP)	Filters networks received in updates.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list description	Adds a text description of a prefix list.
ip prefix-list sequence-number	Enables the generation of sequence numbers for entries in a prefix list.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
show ip bgp regexp	Displays information about a prefix list or prefix list entries.

continue

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

continue [*sequence-number*]

no continue

Syntax Description

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

Defaults

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

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

Command Modes

Route-map configuration (config-route-map)

Command History

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

Usage Guidelines

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

Route Map Operation Without Continue Clauses

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

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

Route Map Operation With Continue Clauses

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

Match Operations With Continue Clauses

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

Set Operations With Continue Clauses

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



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

Examples

In the following example, continue clause configuration is shown.

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

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

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

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

Related Commands

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

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

default-information originate (BGP)

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

default-information originate

no default-information originate

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Address family configuration
Router configuration

Command History

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

Usage Guidelines

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

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



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

Examples

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

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

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

Related Commands

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

default-metric (BGP)

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

default-metric *number*

no default-metric *number*

Syntax Description

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

Defaults

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

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

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

Command Modes

Address family configuration
Router configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

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

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

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

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

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

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

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

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

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

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

Total number of prefixes 2
```

Related Commands

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

distance bgp

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

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

no distance bgp

Syntax Description

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

Defaults

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

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

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

Command Modes

Address family configuration
Router configuration

Command History

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

Usage Guidelines

The **distance bgp** command is used to configure a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is a positive integer from 1 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should

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

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

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

Examples

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

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

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.

distribute-list in (BGP)

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Router configuration

Command History

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

Usage Guidelines

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



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

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

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

Examples

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

```
Router(config)# ip prefix-list RED permit 10.1.1.0/24
Router(config)# ip prefix-1ist RED permit 10.108.0.0/16
Router(config)# ip prefix-list RED permit 192.168.1.0/24
Router(config)# router bgp 50000
Router(config-router)# network 10.108.0.0
Router(config-router)# distribute-list prefix RED in
Router(config-router)# end
Router# clear ip bgp in
```

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

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

Related Commands

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

distribute-list out (BGP)

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Router configuration

Command History

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

Usage Guidelines

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

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

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

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

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

Examples

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

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

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

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

Related Commands

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

exit-peer-policy

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

exit-peer-policy

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

Policy-template configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

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

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

Related Commands

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

exit-peer-session

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

exit-peer-session

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Session-template configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

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

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

Related Commands

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

export map

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

export map *route-map*

no export map *route-map*

Syntax Description

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

Command Default

No export maps are associated with a VRF instance.

Command Modes

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

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

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

Related Commands

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

ha-mode graceful-restart

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

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

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

Syntax Description

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

Command Default

BGP graceful restart is disabled.

Command Modes

Peer session template configuration (config-router-stmp)

Command History

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

Usage Guidelines

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

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

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

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

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

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

Examples

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

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

Related Commands

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

import ipv4

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

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

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

Syntax Description

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

Command Default

No import map is configured.

Command Modes

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

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

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

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

No MPLS or Route Target Configuration Is Required

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

Import Behavior

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

Examples

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

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

Related Commands

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

import path limit

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

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

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

Syntax Description

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

Command Default

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

Command Modes

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

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

import path selection

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

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

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

Syntax Description

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

Command Default

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

Command Modes

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

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

Command	Description
import path limit	Specifies the maximum number of BGP paths, per VRF importing net, that can be imported from an exporting net.
show ip bgp vpnv4	Displays VPNv4 address information from the BGP table.

inherit peer-policy

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

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

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

Syntax Description

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

Defaults

No inherit statements are configured.

Command Modes

Policy-template configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **inherit peer-policy** command is used to configure a peer policy template to inherit the configuration of another peer policy template. Peer policy templates support inheritance and a peer can directly and indirectly inherit up to seven peer policy templates. Inherited peer policy templates are configured with sequence numbers like route maps. An inherited peer policy template, like a route map, is evaluated starting with the inherit statement with the lowest sequence number. However, peer policy templates do not fall through. Every sequence is evaluated. If a BGP policy command is reapplied with a different value, it will overwrite any previous value from a lower sequence number.



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

Examples

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

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

Related Commands

Command	Description
exit peer-policy	Exits policy-template configuration mode and enters router configuration mode.
neighbor inherit peer-policy	Configures a router to send a peer policy template to a neighbor so that the neighbor can inherit the configuration.
show ip bgp template peer-policy	Displays locally configured peer policy templates.
template peer-policy	Creates a peer policy template and enters policy-template configuration mode.

inherit peer-session

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

inherit peer-session *template-name*

no inherit peer-session *template-name*

Syntax Description

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

Defaults

No inherit statements are configured.

Command Modes

Session-template configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

Command	Description
exit peer-session	Exits session-template configuration mode and enters router configuration mode.
neighbor inherit peer-session	Configures a router to send a peer session template to a neighbor so that the neighbor can inherit the configuration.
show ip bgp template peer-session	Displays locally configured peer session templates.
template peer-session	Creates a peer session template and enters session-template configuration mode.

ip as-path access-list

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

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

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

Syntax Description

acl-number	Number from 1 to 500 that specifies the AS-path access-list number.
permit	Permits advertisement based on matching conditions.
deny	Denies advertisement based on matching conditions.
regexp	Regular expression that defines the AS-path filter. The autonomous system number is expressed in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command. **Note** See the "Regular Expressions" appendix in the *Cisco IOS Terminal Services Configuration Guide* for information about configuring regular expressions.

Command Default

No autonomous system path filter is created.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	This command was modified. The range of values that can be entered for the *acl-number* argument was increased from 199 to 500 in Cisco IOS Release 12.0(22)S.
12.2(15)T	This command was modified. The range values that can be entered for the *acl-number* argument was increased from 199 to 500 in Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

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

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

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

Examples

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

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

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

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

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

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, shows BGP path filtering by neighbor using 4-byte autonomous system numbers in asplain format. Only the routes that pass autonomous system path access list 2 will be sent to 192.168.3.2.

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

The following example shows BGP path filtering by neighbor using 4-byte autonomous system numbers in asdot format. The dot notation is the only format for 4-byte autonomous system numbers in Cisco IOS Release 12.0(32)S12, 12.4(24)T, or Cisco IOS XE Release 2.3. This example can also be configured using Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or later releases. after the **bgp asnotation dot** command has been entered to allow matching of 4-byte autonomous system numbers in regular expressions in asdot notation. The dot in the asdot notation is a special character for regular expressions and a backslash must precede it, as shown in the example. Only the routes that pass autonomous system path access list 2 will be sent to 192.168.3.2.

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

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
neighbor distribute-list	Distributes BGP neighbor information as specified in an access list.
neighbor filter-list	Applies a filter list to the specified neighbor.
neighbor prefix-list	Applies a prefix list to the specified neighbor.
router bgp	Configures the BGP routing process.

ip bgp fast-external-fallover

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The **ip bgp fast-external-fallover** command is used to configure per-interface fast external fallover, overriding the global configuration. Entering the **permit** keyword enables fast external fallover. Entering the **deny** keyword disables fast external fallover. Entering the **no** form of this command, returns the router to the global configuration.

Examples

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

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

Related Commands

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

ip bgp-community new-format

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

ip bgp-community new-format

no ip bgp-community new-format

Syntax Description

This command has no argument or keywords.

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

```
Router# show ip bgp 10.0.0.0

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

Related Commands

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

ip community-list

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

Standard Community Lists

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

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

Expanded Community Lists

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

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

Syntax Description

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

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

Command Default

BGP community exchange is not enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.0	Support for the **local-as** community was introduced.
12.0(10)S	Named community list support was added.
12.0(16)ST	Named community list support was introduced.
12.1(9)E	Named community list support was integrated into Cisco IOS Release 12.1(9)E.
12.2(8)T	Named community list support was integrated into Cisco IOS Release 12.2(8)T.
12.0(22)S	The maximum number of expanded community list numbers was increased from 199 to 500.
12.2(14)S	The maximum number of expanded community list numbers was increased from 199 to 500 and named community list support were integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	The maximum number of expanded community list numbers was increased from 199 to 500.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip community-list** command is used to configure BGP community filtering. BGP community values are configured as a 32-bit number (old format) or as a 4-byte number (new format). The new community format is enabled when the **ip bgp-community new-format** command is entered in global configuration mode. The new community format consists of a 4-byte value. The first two bytes represent the autonomous system number, and the trailing two bytes represent a user-defined network number. Named and numbered community lists are supported. BGP community attribute exchange between BGP peers is enabled when the **neighbor send-community** command is configured for the specified neighbor. The BGP community attribute is defined in RFC 1997 and RFC 1998.

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

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

Standard Community Lists

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

Expanded Community Lists

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

Community List Processing

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

Examples

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

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

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

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

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

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

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

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

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

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

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

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

Related Commands

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

ip extcommunity-list

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

Global Configuration Mode CLI

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

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

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

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

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

Expanded IP Extended Community-List Configuration Mode CLI

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

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

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

Standard IP Extended Community-List Configuration Mode CLI

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

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

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

Syntax Description

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

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

Command Default

Extended community exchange is not enabled by default.

Command Modes

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

Command History

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

Release	Modification
12.2(25)S	Support for the following was added in Cisco IOS Release 12.2(25)S: • Extended community-list sequencing • IP Extended community configuration mode • Named extended community lists
12.3(11)T	Support for the following was added in Cisco IOS Release 12.3(11)T: • Extended community-list sequencing • IP Extended community configuration mode • Named extended community lists
12.2(27)SBC	This command was integrated into the Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	This command was integrated into the Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

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

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

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

Route Target Extended Community Attribute

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

Site of Origin Extended Community Attribute

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

IP Extended Community-List Configuration Mode

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

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

Extended Community List Processing

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

Examples

Standard Extended Community-List Configuration Example

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

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

Expanded Extended Community-List Configuration Example

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

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

Named Extended Community-List Configuration Example

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

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

IP Extended Community-List Configuration Mode Example

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

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

Extended Community-List Resequencing Example

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

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

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

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

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

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

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

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

Related Commands

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

ip policy-list

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

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

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

Syntax Description

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

Defaults

This command is not enabled by default.

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

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

Examples

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

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

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

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

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

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

Related Commands

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

ip prefix-list

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

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

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

Syntax Description

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

Command Default

No prefix lists or prefix-list entries are created.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

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

The following formula shows this behavior:

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

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

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

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

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

Related Commands

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

ip prefix-list description

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

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

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

Syntax Description

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

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

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

ip prefix-list sequence-number

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

ip prefix-list sequence-number

no ip prefix-list sequence-number

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Global configuration

Command History

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

Examples

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

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

Related Commands

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

ip verify unicast vrf

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

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

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

Syntax Description

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

Command Default

Unicast RPF verification is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

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

Examples

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

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

Related Commands

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

match as-path

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

match as-path *path-list-number*

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

Syntax Description

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

Defaults

No path lists are defined.

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

The values set by the **match as-path** and **set weight** commands override global values. For example, the weights assigned with the **match as-path** and **set weight** route-map configuration commands override the weight assigned using the **neighbor weight** command.

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

Examples

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

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

Related Commands

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

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

match community

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

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

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

Syntax Description

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

Command Default

No community list is matched by the route map.

Command Modes

Route-map configuration

Command History

Release	Modification
12.1	This command was introduced.
12.1(9)E	Named community list support was integrated into Cisco IOS Release 12.1(9)E.
12.2(8)T	Named community list support was integrated into Cisco IOS Release 12.2(8)T.
12.0(22)S	The maximum number of expanded extended community list numbers was changed from 199 to 500 in Cisco IOS Release 12.0(22)S.
12.2(14)S	The maximum number of expanded community lists was changed from 199 to 500 and named community list support were integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	The maximum number of expanded extended community list numbers was changed from 199 to 500 in Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

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

Examples

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

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

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

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

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

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

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

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

Related Commands

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

match extcommunity

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

match extcommunity *extended-community-list-name*

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

Syntax Description

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

Command Default

BGP and EIGRP extended community list attributes are not matched.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.1	This command was introduced.
12.0(22)S	The maximum number of expanded extended community list numbers was changed from 199 to 500 in Cisco IOS Release 12.0(22)S.
12.2(15)T	The maximum number of expanded extended community list numbers was changed from 199 to 500 in Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. Support for EIGRP was added.
12.2(33)SRE	This command was modified. Support for EIGRP was added.
Cisco IOS XE Release 2.5	This command was modified. Support for EIGRP was added.
12.2(33)XNE	This command was modified. Support for EIGRP was added.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

match local-preference

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

match local-preference *value*

no match local-preference *value*

Syntax Description

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

Command Default

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

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

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

Redistributing OER Injected Routes

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

Examples

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

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

Related Commands

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

match policy-list

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

match policy-list *policy-list-name*

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

Syntax Description

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

Defaults

This command is not enabled by default.

Command Modes

Route-map configuration

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

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

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

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

Related Commands

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

match source-protocol

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

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

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

Syntax Description

source-protocol	Protocol to match. The valid keywords are **bgp**, **connected**, **eigrp, isis**, **ospf**, **rip**, and **static**. There is no default.
autonomous-system-number	(Optional) Autonomous system number. This argument is not applicable to the **connected**, **rip**, and **static** keywords. The range is from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command.

Command Default

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

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.

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

Usage Guidelines

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

Examples

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

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

The following example shows how to configure a route map to match a source protocol of BGP and a 4-byte autonomous system of 65538 in asplain format. When the match clause is true, the tag value of the destination routing protocol is set to 5. The route map is used to distribute incoming packets for an EIGRP process. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

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

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

Release 2.3 where asdot notation is the only format for 4-byte autonomous system numbers. This configuration can also be performed using Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

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

Related Commands

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

maximum-paths eibgp

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Address family configuration (config-router-af)

Command History

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

Usage Guidelines

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

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

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

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

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

Configuring VRF Import Paths

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

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

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

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

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

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

Examples

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

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

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

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

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

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

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

Related Commands

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

maximum-paths ibgp

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

Router Configuration Mode

maximum-paths ibgp *number-of-paths*

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

Under VRF in Address Family Configuration Mode

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

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

Syntax Description

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

Command Default

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

Command Modes

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

Command History

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

Release	Modification
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.3	The **import** keyword was added.
12.3(2)T	The maximum number of parallel routes was increased from 6 to 16.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S for use in IPv6.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was modified. The **import** keyword was replaced by the **import path selection** and **import path limit** commands.
12.2(33)SRE	This command was modified. The **import** keyword was replaced by the **import path selection** and **import path limit** commands.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

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

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

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

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

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

Configuring VRF Import Paths

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

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

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



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

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

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

Examples

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

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

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

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

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

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

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

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

Related Commands

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

neighbor activate

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

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

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

Syntax Description

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

Command Default

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

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

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0(5)T	Support for address family configuration mode and the IPv4 address family was added.
12.2(2)T	The *ipv6-address* argument and support for the IPv6 address family were added.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **%** keyword was added

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

Usage Guidelines

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

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

Examples

Address Exchange Example for Address Family vpn4

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

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

Address Exchange Example for Address Family IPv4 Unicast

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

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

Address Exchange Example for Address Family IPv6

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

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

Related Commands

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

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

neighbor advertise-map

To install a Border Gateway Protocol (BGP) route as a locally originated route in the BGP routing table for conditional advertisement, use the **neighbor advertise-map** command in router configuration mode. To disable conditional advertisement, use the **no** form of this command.

neighbor *ip-address* **advertise-map** *map-name* {**exist-map** *map-name* | **non-exist-map** *map-name*}

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

Syntax Description

ip-address	Specifies the IP address of the router that should receive conditional advertisements.
advertise-map *map-name*	Specifies the name of the route map that will be advertised if the conditions of the exist map or nonexist map are met.
exist-map *map-name*	Specifies the name of the route map that will be compared to the advertise map. If the condition is met and a match occurs between the advertise map and exist map, the route will be advertised. If no match occurs, then the condition is not met, and the route is withdrawn.
non-exist-map *map-name*	Specifies the name of the route map that will be compared to the advertise map. If the condition is met and no match occurs, the route will be advertised. If a match occurs, then the condition is not met, and the route is withdrawn.

Defaults

No default behavior or values

Command Modes

Router configuration

Command History

Release	Modification
11.1CC	This command was introduced.
11.2	This command was integrated into Cisco IOS Release 11.2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **neighbor advertise-map** router configuration command to conditionally advertise selected routes. The routes or prefixes that will be conditionally advertised are defined in 2 route-maps, an advertise map and an exist map or nonexist map. The route map associated with the exist map or nonexist map specifies the prefix that the BGP speaker will track. The route map associated with the advertise-map specifies the prefix that will be advertised to the specified neighbor when the condition is met. When configuring an exist map, the condition is met when the prefix exists in both the advertise map and the exist map. When

configuring a nonexist map, the condition is met when the prefix exists in the advertise map but does not exist in the nonexist map. If the condition is not met, the route is withdrawn and conditional advertisement does not occur. All routes that may be dynamically advertised or not advertised need to exist in the BGP routing table for conditional advertisement to occur.

Examples

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

```
router bgp 5
 neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
```

The following address family configuration example configures BGP to conditionally advertise a prefix to the 10.1.1.1 neighbor using a nonexist map. If the prefix exists in MAP3 but not MAP4, the condition is met and the prefix is advertised.

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

Related Commands

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

neighbor advertisement-interval

To set the minimum route advertisement interval (MRAI) between the sending of BGP routing updates, use the **neighbor advertisement-interval** command in address family or router configuration mode. To restore the default value, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds*

no neighbor {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds*

Syntax Description

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

Defaults

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

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4T, 12.2SB, 12.2SE, 12.2SG, 12.2SR, 12.2SX, Cisco IOS XE 2.1	This command was modified. The default value for eBGP sessions in a VRF and for iBGP sessions changed from .5 seconds to 0 seconds.

Usage Guidelines

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

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

Examples

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

```
router bgp 5
 neighbor 10.4.4.4 advertisement-interval 10
```

The following address family configuration mode example sets the minimum time between sending BGP routing updates to 10 seconds:

```
router bgp 5
address-family ipv4 unicast
 neighbor 10.4.4.4 advertisement-interval 10
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
neighbor peer-group (creating)	Creates a BGP peer group.

neighbor capability orf prefix-list

To advertise outbound route filter (ORF) capabilities to a peer router, use the **neighbor capability orf prefix-list** command in address family or router configuration mode. To disable ORF capabilities, use the **no** form of this command.

neighbor *ip-address* **capability orf prefix-list** [**receive** | **send** | **both**]

no neighbor *ip-address* **capability orf prefix-list** [**receive** | **send** | **both**]

Syntax Description

ip-address	The IP address of the neighbor router.
receive	(Optional) Enables the ORF prefix list capability in receive mode.
send	(Optional) Enables the ORF prefix list capability in send mode.
both	(Optional) Enables the ORF prefix list capability in both receive and send modes.

Command Default

No ORF capabilities are advertised to a peer router.

Command Modes

Address family

Command History

Release	Modification
12.0(11)ST	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **neighbor capability orf prefix-list** command is used to reduce the number of BGP prefixes that a BGP speaker sends or receives from a peer router based on prefix filtering.

In most configurations, this command will be used to advertise both send and receive ORF capabilities with the **both** keyword. However, this feature can be configured in one direction between two routers with one router configured to send ORF capabilities and another router configured to receive ORF capabilities from the first router.

Examples

The following examples configure routers to advertise ORF send or receive capabilities to BGP neighbors.

Router-A Configuration (Sender)

The following example creates an outbound route filter and configures Router-A (10.1.1.1) to advertise the filter to Router-B (172.16.1.2). An IP prefix list named FILTER is created to specify the 192.168.1.0/24 subnet for outbound route filtering. The ORF send capability is configured on Router-A so that Router-A can advertise the outbound route filter to Router-B.

```
ip prefix-list FILTER seq 10 permit 192.168.1.0/24
!
router bgp 100
 address-family ipv4 unicast
 neighbor 172.16.1.2 remote-as 200
 neighbor 172.16.1.2 ebgp-multihop
 neighbor 172.16.1.2 capability orf prefix-list send
 neighbor 172.16.1.2 prefix-list FILTER in
 exit
```

Router-B Configuration (Receiver)

The following example configures Router-B to advertise the ORF receive capability to Router-A. Router-B will install the outbound route filter, defined in the FILTER prefix list, after ORF capabilities have been exchanged. An inbound soft reset is initiated on Router-B at the end of this configuration to activate the outbound route filter.

```
router bgp 200
 address-family ipv4 unicast
 neighbor 10.1.1.1 remote-as 100
 neighbor 10.1.1.1 ebgp-multihop 255
 neighbor 10.1.1.1 capability orf prefix-list receive
 end
clear ip bgp 10.1.1.1 in prefix-filter
```

Note The inbound soft refresh must be initiated with the **clear ip bgp** command in order for the BGP ORF feature to function.

Related Commands

Command	Description
neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.

neighbor default-originate

To allow a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route, use the **neighbor default-originate** command in address family or router configuration mode. To send no route as a default, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*]

no neighbor {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*]

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
route-map *map-name*	(Optional) Name of the route map. The route map allows route 0.0.0.0 to be injected conditionally.

Defaults

No default route is sent to the neighbor.

Command Modes

Address family
Router configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0	Modifications were added to permit extended access lists.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command does not require the presence of 0.0.0.0 in the local router. When used with a route map, the default route 0.0.0.0 is injected if the route map contains a **match ip address** clause and there is a route that matches the IP access list exactly. The route map can contain other match clauses also.

You can use standard or extended access lists with the **neighbor default-originate** command.

Examples

In the following router configuration example, the local router injects route 0.0.0.0 to the neighbor 172.16.2.3 unconditionally:

```
router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 200
 neighbor 172.16.2.3 default-originate
```

In the following example, the local router injects route 0.0.0.0 to the neighbor 172.16.2.3 only if there is a route to 192.168.68.0 (that is, if a route with any mask exists, such as 255.255.255.0 or 255.255.0.0):

```
router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 200
 neighbor 172.16.2.3 default-originate route-map default-map
!
route-map default-map 10 permit
 match ip address 1
!
access-list 1 permit 192.168.68.0
```

In the following example, the last line of the configuration has been changed to show the use of an extended access list. The local router injects route 0.0.0.0 to the neighbor 172.16.2.3 only if there is a route to 192.168.68.0 with a mask of 255.255.0.0:

```
router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 200
 neighbor 172.16.2.3 default-originate route-map default-map
!
route-map default-map 10 permit
 match ip address 100
!
access-list 100 permit ip host 192.168.68.0 host 255.255.0.0
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
neighbor ebgp-multihop	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.

neighbor description

To associate a description with a neighbor, use the **neighbor description** command in router configuration mode or address family configuration mode. To remove the description, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **description** *text*

no neighbor {*ip-address* | *peer-group-name*} **description** [*text*]

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of an EIGRP peer group. This argument is not available in address-family configuration mode.
text	Text (up to 80 characters in length) that describes the neighbor.

Command Default

There is no description of the neighbor.

Command Modes

Router configuration (config-router)
Address family configuration (config-router-af)

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. Address-family configuration mode was added.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Examples

In the following examples, the description of the neighbor is “peer with example.com”:

```
Router(config)# router bgp 109
Router(config-router)# network 172.16.0.0
Router(config-router)# neighbor 172.16.2.3 description peer with example.com
```

In the following example, the description of the address family neighbor is “address-family-peer”:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 172.16.0.0
Router(config-router-af)# neighbor 172.16.2.3 description address-family-peer
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address family configuration mode to configure an EIGRP routing instance.
network (EIGRP)	Specifies the network for an EIGRP routing process.
router eigrp	Configures the EIGRP address family process.

neighbor disable-connected-check

To disable connection verification to establish an eBGP peering session with a single-hop peer that uses a loopback interface, use the **neighbor disable-connected-check** command in address family or router configuration mode. To enable connection verification for eBGP peering sessions, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **disable-connected-check**

no neighbor {*ip-address* | *peer-group-name*} **disable-connected-check**

Syntax Description

ip-address	IP address of a neighbor.
peer-group-name	Name of a BGP peer group.

Command Default

A BGP routing process will verify the connection of single-hop eBGP peering session (TTL=254) to determine if the eBGP peer is directly connected to the same network segment by default. If the peer is not directly connected to same network segment, connection verification will prevent the peering session from being established.

Command Modes

Address family
Router configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The **neighbor disable-connected-check** command is used to disable the connection verification process for eBGP peering sessions that are reachable by a single hop but are configured on a loopback interface or otherwise configured with a non-directly connected IP address.

This command is required only when the **neighbor ebgp-multihop** command is configured with a TTL value of 1. The address of the single-hop eBGP peer must be reachable. The **neighbor update-source** command must be configured to allow the BGP routing process to use the loopback interface for the peering session.

Examples

In the following example, a single-hop eBGP peering session is configured between two BGP peers that are reachable on the same network segment through a local loopback interfaces on each router:

BGP Peer 1

```
Router(config)# interface loopback 1
Router(config-if)# ip address 10.0.0.100 255.255.255
Router(config-if)# exit
Router(config)# router bgp 64512
Router(config-router)# neighbor 192.168.0.200 remote-as 65534
```

```
Router(config-router)# neighbor 192.168.0.200 ebgp-multihop 1
Router(config-router)# neighbor 192.168.0.200 update-source loopback 2
Router(config-router)# neighbor 192.168.0.200 disable-connected-check
Router(config-router)# end
```

BGP Peer 2

```
Router(config)# interface loopback 2
Router(config-if)# ip address 192.168.0.200 255.255.255
Router(config-if)# exit
Router(config)# router bgp 65534
Router(config-router)# neighbor 10.0.0.100 remote-as 64512
Router(config-router)# neighbor 10.0.0.100 ebgp-multihop 1
Router(config-router)# neighbor 10.0.0.100 update-source loopback 1
Router(config-router)# neighbor 10.0.0.100 disable-connected-check
Router(config-router)# end
```

Related Commands

Command	Description
neighbor ebgp-multihop	Accepts or initiates BGP connections to external peers residing on networks that are not directly connected.
neighbor update-source	Configures Cisco IOS software to allow BGP sessions to use any operational interface for TCP connections.

neighbor distribute-list

To distribute BGP neighbor information as specified in an access list, use the **neighbor distribute-list** command in address family or router configuration mode. To remove an entry, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **distribute-list** {*access-list-number* | *expanded-list-number* | *access-list-name*| *prefix-list-name*} {**in** | **out**}

no neighbor {*ip-address* | *peer-group-name*} **distribute-list** {*access-list-number* | *expanded-list-number* | *access-list-name*| *prefix-list-name*} {**in** | **out**}

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
access-list-number	Number of a standard or extended access list. The range of a standard access list number is from 1 to 99. The range of an extended access list number is from 100 to 199.
expanded-list-number	Number of an expanded access list number. The range of an expanded access list is from 1300 to 2699.
access-list-name	Name of a standard or extended access list.
prefix-list-name	Name of a BGP prefix list.
in	Access list is applied to incoming advertisements to that neighbor.
out	Access list is applied to outgoing advertisements to that neighbor.

Defaults

No BGP neighbor is specified.

Command Modes

Address family
Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The *peer-group-name* argument was added.
11.2	The *access-list-name* argument was added.
12.0	The *prefix-list-name* argument was added.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

Using a distribute list is one of several ways to filter advertisements. Advertisements can also be filtered by using the following methods:

- Autonomous system path filters can be configured with the **ip as-path access-list** and **neighbor filter-list** commands.
- The **access-list (IP standard)** and **access-list (IP extended)** commands can be used to configure standard and extended access lists for the filtering of advertisement.
- The **route-map (IP)** command can be used to filter advertisements. Route maps may be configured with autonomous system filters, prefix filters, access lists and distribute lists.

Standard access lists may be used to filter routing updates. However, in the case of route filtering when using classless interdomain routing (CIDR), standard access lists do not provide the level of granularity that is necessary to configure advanced filtering of network addresses and masks. Extended access lists, configured with the **access-list (IP extended)** command, should be used to configure route filtering when using CIDR because extended access lists allow the network operator to use wild card bits to filter the relevant prefixes and masks. Wild card bits are similar to the bit masks that are used with normal access lists; prefix and mask bits that correspond to wild card bits that are set to 0 are used in the comparison of addresses or prefixes and wild card bits that are set to 1 are ignored during any comparisons. This function of extended access list configuration can also be used to filter addresses or prefixes based on the prefix length.

Note Do not apply both a **neighbor distribute-list** and a **neighbor prefix-list** command to a neighbor in any given direction (inbound or outbound). These two commands are mutually exclusive, and only one command (**neighbor prefix-list** or **neighbor distribute-list**) can be applied to each inbound or outbound direction.

Examples

The following router configuration mode example applies list 39 to incoming advertisements from neighbor172.16.4.1. List 39 permits the advertisement of network 10.109.0.0.

```
router bgp 109
 network 10.108.0.0
 neighbor 172.16.4.1 distribute-list 39 in
```

The following three examples show different scenarios for using an extended access list with a distribute list. The three examples are labeled “Example A”, “Example B”, and “Example C.” Each of the example extended access list configurations are used with the **neighbor distribute-list** command configuration example below.

```
router bgp 109
 network 10.108.0.0
 neighbor 172.16.4.1 distribute-list 101 in
```

Example A

The following extended access list example will permit route 192.168.0.0 255.255.0.0 but deny any more specific routes of 192.168.0.0 (including 192.168.0.0 255.255.255.0):

```
access-list 101 permit ip 192.168.0.0 0.0.0.0 255.255.0.0 0.0.0.0
access-list 101 deny ip 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

Example B

The following extended access list example will permit route 10.108.0/24 but deny 10.108/16 and all other subnets of 10.108.0.0:

```
access-list 101 permit ip 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0
access-list 101 deny ip 10.108.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

Example C

The following extended access list example will deny all prefixes that are longer than 24 bits and permit all of the shorter prefixes:

```
access-list 101 deny ip 0.0.0.0 255.255.255.255 255.255.255.0 0.0.0.255
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
ip as-path access-list	Defines a BGP-related access list.
neighbor filter-list	Sets up a BGP filter.
neighbor peer-group (creating)	Creates a BGP peer group.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.

neighbor dmzlink-bw

To configure Border Gateway Protocol (BGP) to advertise the bandwidth of links that are used to exit an autonomous system, use the **neighbor dmzlink-bw** command in address family configuration mode. To disable the link bandwidth advertisement, use the **no** form of this command.

neighbor *ip-address* **dmzlink-bw**

no neighbor *ip-address* **dmzlink-bw**

Syntax Description

ip-address	IP address of the neighbor router for which the bandwidth of the outbound link is advertised.

Command Default

This command is disabled by default.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **neighbor dmzlink-bw** command is used to configure BGP to advertise the bandwidth of the specified external interface as an extended community. This command is configured for links between directly connected external BGP (eBGP) neighbors. The link bandwidth extended community attribute is propagated to iBGP peers when extended community exchange is enabled with the **neighbor send-community** command. This feature is used with BGP multipath features to configure load balancing over links with unequal bandwidth. This feature is not enabled until the **bgp dmzlink-bw** command is entered under the address family session for each router that has a directly connected external link.

Examples

In the following example, the BGP Link Bandwidth feature is configured to allow multipath load balancing to distribute link traffic proportionally to the bandwidth of each external link, and to advertise the bandwidth of these links to iBGP peers as an extended community:

```
Router(config)# router bgp 100
Router(config-router)# neighbor 10.10.10.1 remote-as 100
Router(config-router)# neighbor 10.10.10.1 update-source Loopback 0
Router(config-router)# neighbor 10.10.10.3 remote-as 100
```

```
Router(config-router)# neighbor 10.10.10.3 update-source Loopback 0
Router(config-router)# neighbor 172.16.1.1 remote-as 200
Router(config-router)# neighbor 172.16.1.1 ebgp-multihop 1
Router(config-router)# neighbor 172.16.2.2 remote-as 200
Router(config-router)# neighbor 172.16.2.2 ebgp-multihop 1
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp dmzlink-bw
Router(config-router-af)# neighbor 10.10.10.1 activate
Router(config-router-af)# neighbor 10.10.10.1 next-hop-self
Router(config-router-af)# neighbor 10.10.10.1 send-community both
Router(config-router-af)# neighbor 10.10.10.3 activate
Router(config-router-af)# neighbor 10.10.10.3 next-hop-self
Router(config-router-af)# neighbor 10.10.10.3 send-community both
Router(config-router-af)# neighbor 172.16.1.1 activate
Router(config-router-af)# neighbor 172.16.1.1 dmzlink-bw
Router(config-router-af)# neighbor 172.16.2.2 activate
Router(config-router-af)# neighbor 172.16.2.2 dmzlink-bw
Router(config-router-af)# maximum-paths ibgp 6
Router(config-router-af)# maximum-paths 6
```

Related Commands

Command	Description
bgp dmzlink-bw	Configures BGP to distribute traffic proportionally over external links with unequal bandwidth when multipath load balancing is enabled.
neighbor send-community	Specifies that a communities attribute should be sent to a BGP neighbor.

neighbor ebgp-multihop

To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the **neighbor ebgp-multihop** command in router configuration mode. To return to the default, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop**

Syntax Description

ip-address	IP address of the BGP-speaking neighbor.
ipv6-address	IPv6 address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
ttl	(Optional) Time-to-live in the range from 1 to 255 hops.

Command Default

Only directly connected neighbors are allowed.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The *peer-group-name* argument was added.
12.2(33)SRA	The *ipv6-address* argument and support for the IPv6 address family were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

This feature should be used only under the guidance of Cisco technical support staff.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

To prevent the creation of loops through oscillating routes, the multihop will not be established if the only route to the multihop peer is the default route (0.0.0.0).

Examples

The following example allows connections to or from neighbor 10.108.1.1, which resides on a network that is not directly connected:

```
router bgp 109
 neighbor 10.108.1.1 ebgp-multihop
```

Related Commands

Command	Description
neighbor advertise-map non-exist-map	Allows a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.
neighbor peer-group (creating)	Creates a BGP peer group.
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.

neighbor fall-over

To enable Border Gateway Protocol (BGP) to monitor the peering session of a specified neighbor for adjacency changes and to deactivate the peering session, use the **neighbor fall-over** command in address-family or router configuration mode. To disable BGP monitoring of the neighbor peering session, use the **no** form of this command.

neighbor *ip-address* **fall-over** [**bfd** | **route-map** *map-name*]

no neighbor *ip-address* **fall-over** [**bfd** | **route-map** *map-name*]

Syntax Description

ip-address	IP address of a BGP neighbor.
bfd	(Optional) Enables Bidirectional Forwarding Detection (BFD) protocol support for fallover.
route-map	(Optional) Specifies the use of a route map.
map-name	(Optional) Name of the route map.

Command Default

BGP does not monitor neighbor peering sessions.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.4(4)T	The **route-map** keyword and *map-name* argument were added to support the BGP Selective Address Tracking feature.
12.2(33)SRA	The **bfd** keyword was added to support the BFD feature, and this command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **route-map** keyword and *map-name* argument were added to support the BGP Selective Address Tracking feature.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	The **bfd** keyword was added to support the BFD feature, and this command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **neighbor fall-over** command is a BGP neighbor session command that is used to enable BGP fast peering session deactivation. BGP fast peering session deactivation improves BGP convergence and response time to adjacency changes with BGP neighbors. BGP fast peering session deactivation is event

driven and is configured on a per-neighbor basis. When BGP fast peering session deactivation is enabled, BGP will monitor the peering session with the specified neighbor. Adjacency changes are detected, and terminated peering sessions are deactivated in between the default or configured BGP scanning interval.

In Cisco IOS Release 12.4(4)T, 12.2(33)SRB, and later releases, the optional **route-map** keyword and *map-name* argument are used with this command to determine if a peering session with a BGP neighbor should be deactivated (reset) when a route to the BGP peer changes. The route map is evaluated against the new route, and if a deny statement is returned, the peer session is reset. The route map is not used for session establishment.

Note Only the **match ip address** and **match source-protocol** commands are supported in the route map. No **set** commands or other **match** commands are supported.

In Cisco IOS Release 12.2(33)SRA, 12.2(33)SB, and later releases, the optional **bfd** keyword is used to enable BFD protocol support for fallover. BFD provides fast forwarding path failure detection and a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning will be easier, and reconvergence time will be consistent and predictable. The main benefit of implementing BFD for BGP is a marked decrease in reconvergence time.

Examples

In the following example, the BGP routing process is configured to monitor and use fast peering session deactivation for the neighbor session with the neighbor at 192.168.1.2:

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 fall-over
 end
```

In the following example, the BGP peering session will be reset if a route with a prefix of /28 or a more specific route to a peer destination is no longer available:

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 fall-over route-map CHECK-NBR
 exit
ip prefix-list FILTER28 seq 5 permit 0.0.0.0/0 ge 28
route-map CHECK-NBR permit 10
 match ip address prefix-list FILTER28
 end
```

In the following example, BFD is enabled for the Fast Ethernet interface 0/1 with a specified BFD interval and the BGP peering session is also BFD enabled and this will result in a decreased reconvergence time for BGP if any of the forwarding paths to neighbors fail.

```
interface FastEthernet 0/1
 ip address 172.16.10.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
 exit
router bgp 40000
 bgp log-neighbors-changes
 neighbor 172.16.10.2 remote-as 45000
 neighbor 172.16.10.2 fall-over bfd
 exit
```

Related Commands

Command	Description
bfd interval	Matches IP addresses defined by a prefix list.
match ip address	Matches IP addresses defined by a prefix list.
match source-protocol	Matches the route type based on the source protocol.

neighbor filter-list

To set up a BGP filter, use the **neighbor filter-list** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **filter-list** *access-list-number* {**in** | **out**}

no neighbor {*ip-address* | *peer-group-name*} **filter-list** *access-list-number* {**in** | **out**}

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
access-list-number	Number of an autonomous system path access list. You define this access list with the **ip as-path access-list** command.
in	Access list is applied to incoming routes.
out	Access list is applied to outgoing routes.

Command Default

No BGP filter is used.

Command Modes

Router configuration or Address family configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.1	The **weight** keyword was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command establishes filters on both inbound and outbound BGP routes.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group.

Note Do not apply both a **neighbor distribute-list** and a **neighbor prefix-list** command to a neighbor in any given direction (inbound or outbound). These two commands are mutually exclusive, and only one command (**neighbor distribute-list** or **neighbor prefix-list**) can be applied to each inbound or outbound direction.

Examples

In the following router configuration mode example, the BGP neighbor with IP address 172.16.1.1 is not sent advertisements about any path through or from the adjacent autonomous system 123:

```
ip as-path access-list 1 deny _123_
ip as-path access-list 1 deny ^123$

 router bgp 109
 network 10.108.0.0
 neighbor 192.168.6.6 remote-as 123
 neighbor 172.16.1.1 remote-as 47
 neighbor 172.16.1.1 filter-list 1 out
```

In the following address family configuration mode example, the BGP neighbor with IP address 172.16.1.1 is not sent advertisements about any path through or from the adjacent autonomous system 123:

```
ip as-path access-list 1 deny _123_
ip as-path access-list 1 deny ^123$

router bgp 109
 address-family ipv4 unicast
  network 10.108.0.0
  neighbor 192.168.6.6 remote-as 123
  neighbor 172.16.1.1 remote-as 47
  neighbor 172.16.1.1 filter-list 1 out
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
ip as-path access-list	Defines a BGP-related access list.
match as-path	Matches BGP autonomous system path access lists.
neighbor distribute-list	Distributes BGP neighbor information as specified in an access list.
neighbor peer-group (creating)	Creates a BGP peer group.
neighbor prefix-list	Prevents distribution of BGP neighbor information as specified in a prefix list, a CLNS filter expression, or a CLNS filter set.
neighbor weight	Assigns a weight to a neighbor connection.
set weight	Specifies the BGP weight for the routing table.

neighbor ha-mode graceful-restart

To enable or disable the Border Gateway Protocol (BGP) graceful restart capability for a BGP neighbor or peer group, use the **neighbor ha-mode graceful-restart** command in router configuration mode. To remove from the configuration the BGP graceful restart capability for a neighbor, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **ha-mode graceful-restart** [**disable**]

no neighbor {*ip-address* | *peer-group-name*} **ha-mode graceful-restart** [**disable**]

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
disable	(Optional) Disables BGP graceful restart capability for a neighbor.

Command Default

BGP graceful restart capability is disabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **neighbor ha-mode graceful-restart** command is used to enable or disable the graceful restart capability for an individual BGP neighbor or peer group in a BGP network. Use the **disable** keyword to disable the graceful restart capability when graceful restart has been previously enabled for the BGP peer.

The graceful restart capability is negotiated between nonstop forwarding (NSF)-capable and NSF-aware peers in OPEN messages during session establishment. If the graceful restart capability is enabled after a BGP session has been established, the session will need to be restarted with a soft or hard reset.

The graceful restart capability is supported by NSF-capable and NSF-aware routers. A router that is NSF-capable can perform a stateful switchover (SSO) operation (graceful restart) and can assist restarting peers by holding routing table information during the SSO operation. A router that is NSF-aware functions like a router that is NSF-capable but cannot perform an SSO operation.

To enable the BGP graceful restart capability globally for all BGP neighbors, use the **bgp graceful-restart** command. When the BGP graceful restart capability is configured for an individual neighbor, each method of configuring graceful restart has the same priority, and the last configuration instance is applied to the neighbor.

Use the **show ip bgp neighbors** command to verify the BGP graceful restart configuration for BGP neighbors.

Examples

The following example enables the BGP graceful restart capability for the BGP neighbor, 172.21.1.2:

```
router bgp 45000
 bgp log-neighbor-changes
 address-family ipv4 unicast
 neighbor 172.21.1.2 remote-as 45000
 neighbor 172.21.1.2 activate
 neighbor 172.21.1.2 ha-mode graceful-restart
 end
```

The following example enables the BGP graceful restart capability globally for all BGP neighbors and then disables the BGP graceful restart capability for the BGP peer group PG1. The BGP neighbor 172.16.1.2 is configured as a member of the peer group PG1 and inherits the disabling of the BGP graceful restart capability.

```
router bgp 45000
 bgp log-neighbor-changes
 bgp graceful-restart
 address-family ipv4 unicast
 neighbor PG1 peer-group
 neighbor PG1 remote-as 45000
 neighbor PG1 ha-mode graceful-restart disable
 neighbor 172.16.1.2 peer-group PG1
 end
```

Related Commands

Command	Description
bgp graceful-restart	Enables the BGP graceful restart capability globally for all BGP neighbors.
ha-mode graceful-restart	Enables or disables the BGP graceful restart capability for a BGP peer session template.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

neighbor ha-mode sso

To configure a Border Gateway Protocol (BGP) neighbor to support BGP nonstop routing (NSR) with stateful switchover (SSO), use the **neighbor ha-mode sso** command in the appropriate command mode. To remove the configuration, use the **no** form of this command.

neighbor *ip-address* **ha-mode sso**

no neighbor *ip-address* **ha-mode sso**

Syntax Description

ip-address	IP address of the neighboring router.

Command Default

BGP NSR with SSO support is disabled.

Command Modes

Address family configuration
Session-template configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **neighbor ha-mode sso** command is used to configure a BGP neighbor to support BGP NSR with SSO. BGP NSR with SSO is disabled by default.

BGP NSR with SSO is supported in BGP peer, BGP peer group, and BGP session template configurations. To configure BGP NSR with SSO in BGP peer and BGP peer group configurations, use the **neighbor ha-mode sso** command in address family configuration mode for IPv4 VRF address family BGP peer sessions. To include support for Cisco BGP NSR with SSO in a peer session template, use the **ha-mode sso** command in session-template configuration mode.

Examples

The following example shows how to configure a BGP neighbor to support SSO:

```
Router(config-router-af)# neighbor 10.3.32.154 ha-mode sso
```

Related Commands

Command	Description
show ip bgp vpnv4	Displays VPN address information from the BGP table.
show ip bgp vpnv4 all sso summary	Displays the number of BGP neighbors that support SSO.

neighbor inherit peer-policy

To send a peer policy template to a neighbor so that the neighbor can inherit the configuration, use the **neighbor inherit peer-policy** command in address family or router configuration mode. To stop sending the peer policy template, use the **no** form of this command.

neighbor *ip-address* **inherit peer-policy** *policy-template-name*

no neighbor *ip-address* **inherit peer-policy** *policy-template-name*

Syntax Description

ip-address	IP address of the neighbor.
policy-template-name	Name or tag for the peer policy template.

Defaults

No default behavior or values

Command Modes

Address family
Router configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used to send locally configured policy templates to the specified neighbor. If the policy template is configured to inherit configurations from other peer policy templates, the specified neighbor will also indirectly inherit these configurations from the other peer policy templates. A directly applied peer policy template can directly or indirectly inherit configurations from up to seven peer policy templates. So, a total of eight peer policy templates can be applied to a neighbor or neighbor group.



Note A Border Gateway Protocol (BGP) neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured to belong only to a peer group or to inherit policies only from peer templates.

Examples

The following example configures the 10.0.0.1 neighbor in address family configuration mode to inherit the peer policy template name CUSTOMER-A. The 10.0.0.1 neighbor will also indirectly inherit the peer policy templates in CUSTOMER-A. The explicit remote-as statement is required for the neighbor inherit statement to work. If a peering is not configured, the specified neighbor will not accept the session template.

```
Router(config)# router bgp 101
Router(config-router)# neighbor 10.0.0.1 remote-as 202
Router(config-router)# address-family ipv4 unicast
Router(config-router-af)# neighbor 10.0.0.1 inherit peer-policy CUSTOMER-A
Router(config-router-af)# exit
```

Related Commands

Command	Description
exit peer-policy	Exits policy-template configuration mode and enters router configuration mode.
inherit peer-policy	Configures a peer policy template to inherit the configuration from another peer policy template.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.
show ip bgp template peer-policy	Displays locally configured peer policy templates.
template peer-policy	Creates a peer policy template and enters policy-template configuration mode.

neighbor inherit peer-session

To send a peer session template to a neighbor so that the neighbor can inherit the configuration, use the **neighbor inherit peer-session** command in address family or router configuration mode. To stop sending the peer session template, use the **no** form of this command.

neighbor *ip-address* **inherit peer-session** *session-template-name*

no neighbor *ip-address* **inherit peer-session** *session-template-name*

Syntax Description

ip-address	IP address of the neighbor.
session-template-name	Name or tag for the peer session template.

Defaults

No default behavior or values

Command Modes

Address family
Router configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used to send locally configured session templates to the specified neighbor. If the session template is configured to inherit configurations from other session templates, the specified neighbor will also indirectly inherit these configurations from the other session templates. A neighbor can directly inherit only one peer session template and indirectly inherit up to seven peer session templates.

Note A Border Gateway Protocol (BGP) neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured to belong only to a peer group or to inherit policies only from peer templates.

Examples

The following example configures the 172.16.0.1 neighbor to inherit the CORE1 peer session template. The 172.16.0.1 neighbor will also indirectly inherit the configuration from the peer session template named INTERNAL-BGP. The explicit remote-as statement is required for the neighbor inherit statement to work. If a peering is not configured, the specified neighbor will not accept the session template.

```
Router(config)# router bgp 101
Router(config)# neighbor 172.16.0.1 remote-as 202
Router(config-router)# neighbor 172.16.0.1 inherit peer-session CORE1
```

Related Commands

Command	Description
exit peer-session	Exits session-template configuration mode and enters router configuration mode.
inherit peer-session	Configures a peer session template to inherit the configuration from another peer session template.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.
show ip bgp template peer-session	Displays locally configured peer session templates.
template peer-session	Creates a peer session template and enters session-template configuration mode.

neighbor local-as

To customize the AS_PATH attribute for routes received from an external Border Gateway Protocol (eBGP) neighbor, use the **neighbor local-as** command in address family or router configuration mode. To disable AS_PATH attribute customization, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **local-as** [*autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]]]

no neighbor {*ip-address* | *peer-group-name*} **local-as**

Syntax Description

ip-address	IP address of the eBGP neighbor.
peer-group-name	Name of a BGP peer group.
autonomous-system-number	(Optional) Number of an autonomous system to prepend to the AS_PATH attribute. The range of values for this argument is any valid autonomous system number from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command. **Note** With this argument, you cannot specify the autonomous system number from the local BGP routing process or from the network of the remote peer.
no-prepend	(Optional) Does not prepend the local autonomous system number to any routes received from the eBGP neighbor.
replace-as	(Optional) Replaces the real autonomous system number with the local autonomous system number in the eBGP updates. The autonomous system number from the local BGP routing process is not prepended.
dual-as	(Optional) Configures the eBGP neighbor to establish a peering session using the real autonomous system number (from the local BGP routing process) or by using the autonomous system number configured with the *autonomous-system-number* argument (local-as).

Command Default

The autonomous system number from the local BGP routing process is prepended to all external routes by default.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	CLI support for address family configuration mode was added.
12.2(8)T	The **no-prepend** keyword was added.
12.2(14)S	The **no-prepend** keyword was integrated into Cisco IOS Release 12.2(14)S.
12.0(18)S	The **no-prepend** keyword was integrated into Cisco IOS Release 12.0(18)S.
12.0(27)S	The **replace-as** and **dual-as** keywords were added.
12.2(25)S	The **replace-as** and **dual-as** keywords were integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	The **replace-as** and **dual-as** keywords were integrated into Cisco IOS Release 12.3(11)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

The **neighbor local-as** command is used to customize the AS_PATH attribute by adding and removing autonomous system numbers for routes received from eBGP neighbors. The configuration of this command allows a router to appear to external peers as a member of another autonomous system for the purpose of autonomous system number migration. This feature simplifies the process of changing the autonomous system number in a BGP network by allowing the network operator to migrate customers to new configurations during normal service windows without disrupting existing peering arrangements.

Caution BGP prepends the autonomous system number from each BGP network that a route traverses to maintain network reachability information and to prevent routing loops. This command should be configured only for autonomous system migration, and should be deconfigured after the transition has been completed. This procedure should be attempted only by an experienced network operator. Routing loops can be created through improper configuration.

This command can be used for only true eBGP peering sessions. This command does not work for two peers in different subautonomous systems of a confederation.

This command supports individual peering sessions and configurations applied through peer groups and peer templates. If this command is applied to a group of peers, the individual peers cannot be customized.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

To ensure a smooth transition, we recommend that all BGP speakers within an autonomous system that is identified using a 4-byte autonomous system number, be upgraded to support 4-byte autonomous system numbers.

Examples

local-as Configuration: Example

The following example establishes peering between Router 1 and Router 2 through autonomous system 300, using the local-as feature:

Router 1 (Local Router)

```
router bgp 100
 address-family ipv4 unicast
  neighbor 172.16.1.1 remote-as 200
  neighbor 172.16.1.1 local-as 300
```

Router 2 (Remote Router)

```
router bgp 200
 address-family ipv4 unicast
  neighbor 10.0.0.1 remote-as 300
```

no-prepend Keyword Configuration: Example

The following example configures BGP to not prepend autonomous system 500 to routes received from the 192.168.1.1 neighbor:

```
router bgp 400
 address-family ipv4 multicast
  network 192.168.0.0
  neighbor 192.168.1.1 local-as 500 no-prepend
```

replace-as Keyword Configuration: Example

The following example strips private autonomous system 64512 from outbound routing updates for the 172.20.1.1 neighbor and replaces it with autonomous system 600:

```
router bgp 64512
 address-family ipv4 unicast
  neighbor 172.20.1.1 local-as 600 no-prepend replace-as
  neighbor 172.20.1.1 remove-private-as
```

dual-as Keyword Configuration: Example

The following examples show the configurations for two provider networks and one customer network. Router 1 belongs to autonomous system 100, and Router 2 belongs to autonomous system 200. Autonomous system 200 is being merged into autonomous system 100. This transition needs to occur without interrupting service to Router 3 in autonomous system 300 (customer network). The **neighbor local-as** command is configured on router 1 to allow Router 3 to maintain peering with autonomous system 200 during this transition. After the transition is complete, the configuration on Router 3 can be updated to peer with autonomous system 100 during a normal maintenance window or during other scheduled downtime.

Router 1 Configuration (Local Provider Network)

```
interface Serial3/0
 ip address 10.3.3.11 255.255.255.0
!
router bgp 100
 no synchronization
 bgp router-id 100.0.0.11
 neighbor 10.3.3.33 remote-as 300
 neighbor 10.3.3.33 local-as 200 no-prepend replace-as dual-as
```

Router 2 Configuration (Remote Provider Network)

```
interface Serial3/0
 ip address 10.3.3.11 255.255.255.0
 !
router bgp 200
 bgp router-id 100.0.0.11
 neighbor 10.3.3.33 remote-as 300
```

Router 3 Configuration (Remote Customer Network)

```
interface Serial3/0
 ip address 10.3.3.33 255.255.255.0
 !
router bgp 300
 bgp router-id 100.0.0.3
 neighbor 10.3.3.11 remote-as 200
```

To complete the migration after the two autonomous systems have merged, the peering session is updated on Router 3:

```
neighbor 10.3.3.11 remote-as 100
```

4-Byte Autonomous System Number no-prepend Keyword Configuration: Examples

The following example configures BGP to not prepend the 4-byte autonomous system number of 65536 in asplain format to routes received from the 192.168.1.2 neighbor. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
router bgp 65538
 address-family ipv4 multicast
  network 192.168.0.0
  neighbor 192.168.1.2 local-as 65536 no-prepend
```

The following example configures BGP to not prepend the 4-byte autonomous system number of 1.0 in asdot format to routes received from the 192.168.1.2 neighbor. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, or Cisco IOS XE Release 2.3.

```
router bgp 1.2
 address-family ipv4 multicast
  network 192.168.0.0
  neighbor 192.168.1.2 local-as 1.0 no-prepend
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
neighbor remove-private-as	Removes private autonomous system numbers from outbound routing updates.
router bgp	Configures the BGP routing process.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp neighbors	Displays information about BGP neighbors.

neighbor maximum-prefix

To control how many prefixes can be received from a neighbor, use the **neighbor maximum-prefix** command in router configuration mode. To disable this function, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**warning-only**]

no neighbor {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum*

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
maximum	Maximum number of prefixes allowed from this neighbor.
threshold	(Optional) Integer specifying at what percentage of *maximum* the router starts to generate a warning message. The range is from 1 to 100; the default is 75 (percent).
warning-only	(Optional) Allows the router to generate a log message when the *maximum* is exceeded, instead of terminating the peering.

Defaults

This command is disabled by default. There is no limit on the number of prefixes.

Command Modes

Router configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command allows you to configure a maximum number of prefixes that a BGP router is allowed to receive from a peer. It adds another mechanism (in addition to distribute lists, filter lists, and route maps) to control prefixes received from a peer.

When the number of received prefixes exceeds the maximum number configured, the router terminates the peering (by default). However, if the **warning-only** keyword is configured, the router instead only sends a log message, but continues peering with the sender. If the peer is terminated, the peer stays down until the **clear ip bgp** command is issued.

Examples

The following example sets the maximum number of prefixes allowed from the neighbor at 192.168.6.6 to 1000:

```
router bgp 109
 network 10.108.0.0
 neighbor 192.168.6.6 maximum-prefix 1000
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection using BGP soft reconfiguration.

neighbor maximum-prefix (BGP)

To control how many prefixes can be received from a neighbor, use the **neighbor maximum-prefix** command in router configuration mode. To disable this function, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**]

no neighbor {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum*

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of a Border Gateway Protocol (BGP) peer group.
maximum	Maximum number of prefixes allowed from the specified neighbor. The number of prefixes that can be configured is limited only by the available system resources on a router.
threshold	(Optional) Integer specifying at what percentage of the *maximum*-prefix limit the router starts to generate a warning message. The range is from 1 to 100; the default is 75.
restart	(Optional) Configures the router that is running BGP to automatically reestablish a peering session that has been disabled because the maximum-prefix limit has been exceeded. The restart timer is configured with the *restart-interval* argument.
restart-interval	(Optional) Time interval (in minutes) that a peering session is reestablished. The range is from 1 to 65535 minutes.
warning-only	(optional) Allows the router to generate a sys-log message when the *maximum-prefix limit* is exceeded, instead of terminating the peering session.

Defaults

This command is disabled by default. Peering sessions are disabled when the maximum number of prefixes is exceeded. If the *restart-interval* argument is not configured, a disabled session will stay down after the maximum-prefix limit is exceeded.

threshold: 75 percent

Command Modes

Router configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(22)S	The **restart** keyword was introduced.
12.2(15)T	The **restart** keyword was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	The **restart** keyword was integrated into Cisco IOS Release 12.2(18)S.

Release	Modification
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **neighbor maximum-prefix** command allows you to configure a maximum number of prefixes that a Border Gateway Protocol (BGP) routing process will accept from the specified peer. This feature provides a mechanism (in addition to distribute lists, filter lists, and route maps) to control prefixes received from a peer.

When the number of received prefixes exceeds the maximum number configured, BGP disables the peering session (by default). If the **restart** keyword is configured, BGP will automatically reestablish the peering session at the configured time interval. If the **restart** keyword is not configured and a peering session is terminated because the maximum prefix limit has been exceed, the peering session will not be be reestablished until the **clear ip bgp** command is entered. If the **warning-only** keyword is configured, BGP sends only a log message and continues to peer with the sender.

There is no default limit on the number of prefixes that can be configured with this command. Limitations on the number of prefixes that can be configured are determined by the amount of available system resources.

Examples

In the following example, the maximum prefixes that will be accepted from the 192.168.1.1 neighbor is set to 1000:

```
Router(config)# router bgp 40000
Router(config-router)# network 192.168.0.0
Router(config-router)# neighbor 192.168.1.1 maximum-prefix 1000
```

In the following example, the maximum number of prefixes that will be accepted from the 192.168.2.2 neighbor is set to 5000. The router is also configured to display warning messages when 50 percent of the maximum-prefix limit (2500 prefixes) has been reached.

```
Router(config)# router bgp 40000
Router(config-router)# network 192.168.0.0
Router(config-router)# neighbor 192.168.2.2 maximum-prefix 5000 50
```

In the following example, the maximum number of prefixes that will be accepted from the 192.168.3.3 neighbor is set to 2000. The router is also configured to reestablish a disabled peering session after 30 minutes.

```
Router(config)# router bgp 40000
Router(config-router) network 192.168.0.0
Router(config-router)# neighbor 192.168.3.3 maximum-prefix 2000 restart 30
```

In the following example, warning messages will be displayed when the threshold of the maximum-prefix limit (500 x 0.75 = 375) for the 192.168.4.4 neighbor is exceeded:

```
Router(config)# router bgp 40000
Router(config-router)# network 192.168.0.0
Router(config-router)# neighbor 192.168.4.4 maximum-prefix 500 warning-only
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection using BGP soft reconfiguration.

neighbor next-hop-self

To configure the router as the next hop for a BGP-speaking neighbor or peer group, use the **neighbor next-hop-self** command in router configuration mode. To disable this feature, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **next-hop-self**

no neighbor {*ip-address* | *peer-group-name*} **next-hop-self**

Syntax Description

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The *peer-group-name* argument was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is useful in unmeshed networks (such as Frame Relay or X.25) where BGP neighbors may not have direct access to all other neighbors on the same IP subnet.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group.

For a finer granularity of control, see the **set ip next-hop** command.

Examples

The following example forces all updates destined for 10.108.1.1 to advertise this router as the next hop:

```
router bgp 109
 neighbor 10.108.1.1 next-hop-self
```

Related Commands

Command	Description
neighbor peer-group (creating)	Creates a BGP peer group.
set ip next-hop (BGP)	Indicates where to output packets that pass a match clause of a route map for policy routing.

neighbor next-hop-unchanged

To enable an external BGP (eBGP) multihop peer to propagate the next hop unchanged, use the **neighbor next-hop-unchanged** command in address family or router configuration mode. To disable next hop propagation capabilities, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **next-hop-unchanged** [**allpaths**]

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **next-hop-unchanged** [**allpaths**]

Syntax Description

ip-address	The IP address of the next hop.
ipv6-address	The IPv6 address of the next hop.
peer-group-name	The name of a BGP peer group that is the next hop.
allpaths	(Optional) Unchanged next hop for all paths.

Command Default

Next hop propagation capabilities are not enabled.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(16)ST	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **allpaths** keyword was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **neighbor next-hop-unchanged** command is used to configured the propagate the next hop unchanged for multihop eBGP peering sessions. This command should not be configured on a route reflector, and the **neighbor next-hop-self** command should not be used to modify the next hop attribute for a route reflector when this feature is enabled for a route reflector client.

This command can be used to perform the following tasks:

- Bring the route reflector into the forwarding path, which can be used with the iBGP Multipath Load Sharing feature to configure load balancing.
- Configure interprovider Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) by not modifying the next hop attribute when advertising routes to an eBGP peer.

- Turn off the next hop calculation for an eBGP peer. This feature is useful for configuring the end-to-end connection of a label-switched path.

Caution Incorrectly setting BGP attributes for a route reflector can cause inconsistent routing, routing loops, or a loss of connectivity. Setting BGP attributes for a route reflector should be attempted only by an experienced network operator.

Examples

Route Reflector Configuration

In the following example, the local router is configured as a route reflector and configures the 10.0.0.100 multihop peer as a route reflector client. A route map is created to set the advertised next hop to 172.16.0.1.

```
Router(config)# route-map NEXTHOP
Router(config-route-map)# set ip next-hop 172.16.0.1
Router(config-route-map)# exit
Router(config)# router bgp 65534
Router(config-router)# neighbor 10.0.0.100 remote-as 65412
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 10.0.0.100 activate
Router(config-router-af)# neighbor 10.0.0.100 ebgp-multihop 255
Router(config-router-af)# neighbor 10.0.0.100 route-reflector-client
Router(config-router-af)# neighbor 10.0.0.100 route-map NEXTHOP out
Router(config-router-af)# end
```

Route Reflector Client Configuration

In the following example, the local router (route-reflector client) is configured to establish peering with the route reflector and to propagate the next hop unchanged:

```
Router(config)# router bgp 65412
Router(config-router)# neighbor 192.168.0.1 remote-as 65412
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 192.168.0.1 activate
Router(config-router-af)# neighbor 192.168.0.1 ebgp-multihop 255
Router(config-router-af)# neighbor 192.168.0.1 next-hop-unchanged
Router(config-router-af)# end
```

Related Commands

Command	Description
address-family ipv4	Enters address family configuration mode for configuring routing sessions, such as BGP, RIP, or static routing sessions, that use standard IPv4 address prefixes.
address-family vpnv4	Enters address family configuration mode for configuring routing sessions, such as BGP, RIP, or static routing sessions, that use standard VPNv4 address prefixes.
neighbor ebgp-multihop	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.
neighbor route-map	Applies a route map to incoming or outgoing routes.
neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.

neighbor password

To enable message digest5 (MD5) authentication on a TCP connection between two BGP peers, use the **neighbor password** command in router configuration mode. To disable this function, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **password** *string*

no neighbor {*ip-address* | *peer-group-name*} **password**

Syntax Description

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
string	Case-sensitive password of up to 25 characters in length. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces. You cannot specify a password in the format *number-space-anything*. The space after the number can cause authentication to fail.

Command Default

MD5 is not authenticated on a TCP connection between two BGP peers.

Command Modes

Router configuration (config-router)#

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	This command was integrated into Cisco IOS Release 12.2(24)T. The password was restricted to 25 characters regardless of whether the s**ervice password-encryption** command was enabled.

Usage Guidelines

You can configure MD5 authentication between two BGP peers, meaning that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. Configuring MD5 authentication causes the Cisco IOS software to generate and check the MD5 digest of every segment sent on the TCP connection.

When configuring you can provide a case-sensitive password of up to 25 characters regardless of whether the **service password-encryption** command is enabled . If the length of password is more than 25 characters, an error message is displayed and the password is not accepted. The string can contain any alphanumeric characters, including spaces. A password cannot be configured in the number-space-anything format. The space after the number can cause authentication to fail. You can also use any combination of the following symbolic characters along with alphanumeric characters:

` ~ ! @ # $ % ^ & * ( ) - _ = + | \ }] { [“ ‘ : ; / > < . , ?

Caution If the authentication string is configured incorrectly, the BGP peering session will not be established. We recommend that you enter the authentication string carefully and verify that the peering session is established after authentication is configured.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

If a router has a password configured for a neighbor, but the neighbor router does not, a message such as the following will appear on the console while the routers attempt to establish a BGP session between them:

```
%TCP-6-BADAUTH: No MD5 digest from [peer’s IP address]:11003 to [local router’s
IP address]:179
```

Similarly, if the two routers have different passwords configured, a message such as the following will appear on the screen:

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer’s IP address]:11004 to [local router’s
IP address]:179
```

Configuring an MD5 Password in an Established BGP Session

If you configure or change the password or key used for MD5 authentication between two BGP peers, the local router will not tear down the existing session after you configure the password. The local router will attempt to maintain the peering session using the new password until the BGP hold-down timer expires. The default time period is 180 seconds. If the password is not entered or changed on the remote router before the hold-down timer expires, the session will time out.

Note Configuring a new timer value for the hold-down timer will only take effect after the session has been reset. So, it is not possible to change the configuration of the hold-down timer to avoid resetting the BGP session.

Examples

The following example configures MD5 authentication for the peering session with the 10.108.1.1 neighbor. The same password must be configured on the remote peer before the hold-down timer expires.

```
router bgp 109
 neighbor 10.108.1.1 password bla4u00=2nkq
```

The following example configures a password for more than 25 characters when the **service password-encryption** command is disabled.

```
Router(config)# router bgp 200
Router(config-router)# bgp router-id 2.2.2.2
Router(config-router)# neighbor remote-as 3
Router(config-router)# neighbor 209.165.200.225 password 12345678912345678912345678901
% BGP: Password length must be less than or equal to 25.

Router(config-router)# do show run | i password
no service password-encryption
 neighbor 209.165.200.225 password 123456789123456789123456
```

In the following example an error message occurs when you configure a password for more than 25 characters when the **service password-encryption** command is enabled.

```
Router(config)# service password-encryption
Router(config)# router bgp 200
Router(config-router)# bgp router-id 2.2.2.2
Router(config-router)# neighbor 209.165.200.225 remote-as 3
Router(config-router)# neighbor 209.165.200.225 password 12345678912345678912345678901
% BGP: Password length must be less than or equal to 25.

Router(config-router)# do show run | i password
service password-encryption
 neighbor 209.165.200.225 password 123456789123456789123456
```

Related Commands

Command	Description
neighbor peer-group (creating)	Creates a BGP peer group.
service password-encryption	Encrypts passwords.

neighbor peer-group (assigning members)

To configure a BGP neighbor to be a member of a peer group, use the **neighbor peer-group** command in address family or router configuration mode. To remove the neighbor from the peer group, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address*} **peer-group** *peer-group-name*

no neighbor {*ip-address* | *ipv6-address*} **peer-group** *peer-group-name*

Syntax Description

ip-address	IP address of the BGP neighbor that belongs to the peer group specified by the *peer-group-name argument*.
ipv6-address	IPv6 address of the BGP neighbor that belongs to the peer group specified by the *peer-group-name argument*.
peer-group-name	Name of the BGP peer group to which this neighbor belongs.

Defaults

There are no BGP neighbors in a peer group.

Command Modes

Address family
Router configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(2)T	Support for IPv6 was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The neighbor at the IP address indicated inherits all the configured options of the peer group.

Note Using the **no** form of the **neighbor peer-group** command removes all of the BGP configuration for that neighbor, not just the peer group association.

Examples

The following router configuration mode example assigns three neighbors to the peer group named internal:

```
router bgp 100
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 172.16.232.53 peer-group internal
 neighbor 172.16.232.54 peer-group internal
 neighbor 172.16.232.55 peer-group internal
 neighbor 172.16.232.55 filter-list 3 in
```

The following address family configuration mode example assigns three neighbors to the peer group named internal:

```
router bgp 100
address-family ipv4 unicast
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 172.16.232.53 peer-group internal
 neighbor 172.16.232.54 peer-group internal
 neighbor 172.16.232.55 peer-group internal
 neighbor 172.16.232.55 filter-list 3 in
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
neighbor peer-group (creating)	Creates a BGP peer group.
neighbor shutdown	Disables a neighbor or peer group.

neighbor peer-group (creating)

To create a BGP or multiprotocol BGP peer group, use the **neighbor peer-group** command in address family or router configuration mode. To remove the peer group and all of its members, use the **no** form of this command.

neighbor *peer-group-name* **peer-group**

no neighbor *peer-group-name* **peer-group**

Syntax Description

peer-group-name	Name of the BGP peer group.

Defaults

There is no BGP peer group.

Command Modes

Router configuration

Command History

Release	Modification
11.0	This command was introduced.
11.1(20)CC	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(2)S	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(7)T	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were removed. Address family configuration mode was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Often in a BGP or multiprotocol BGP speaker, many neighbors are configured with the same update policies (that is, same outbound route maps, distribute lists, filter lists, update source, and so on). Neighbors with the same update policies can be grouped into peer groups to simplify configuration and make update calculation more efficient.

Note Peer group members can span multiple logical IP subnets, and can transmit, or pass along, routes from one peer group member to another.

Once a peer group is created with the **neighbor peer-group** command, it can be configured with the **neighbor** commands. By default, members of the peer group inherit all the configuration options of the peer group. Members also can be configured to override the options that do not affect outbound updates.

All the peer group members will inherit the current configuration as well as changes made to the peer group. Peer group members will always inherit the following configuration options by default:

- remote-as (if configured)
- version
- update-source
- outbound route-maps
- outbound filter-lists
- outbound distribute-lists
- minimum-advertisement-interval
- next-hop-self

If a peer group is not configured with a remote-as option, the members can be configured with the **neighbor** {*ip-address* | *peer-group-name*} **remote-as** command. This command allows you to create peer groups containing external BGP (eBGP) neighbors.

Examples

The following example configurations show how to create these types of neighbor peer group:

- internal Border Gateway Protocol (iBGP) peer group
- eBGP peer group
- Multiprotocol BGP peer group

iBGP Peer Group

In the following example, the peer group named internal configures the members of the peer group to be iBGP neighbors. By definition, this is an iBGP peer group because the **router bgp** command and the **neighbor remote-as** command indicate the same autonomous system (in this case, autonomous system 100). All the peer group members use loopback 0 as the update source and use set-med as the outbound route map. The **neighbor internal filter-list 2 in** command shows that, except for 172.16.232.55, all the neighbors have filter list 2 as the inbound filter list.

```
router bgp 100
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 172.16.232.53 peer-group internal
 neighbor 172.16.232.54 peer-group internal
 neighbor 172.16.232.55 peer-group internal
 neighbor 172.16.232.55 filter-list 3 in
```

eBGP Peer Group

The following example defines the peer group named external-peers without the **neighbor remote-as** command. By definition, this is an eBGP peer group because each individual member of the peer group is configured with its respective autonomous system number separately. Thus the peer group consists of

members from autonomous systems 200, 300, and 400. All the peer group members have the set-metric route map as an outbound route map and filter list 99 as an outbound filter list. Except for neighbor 172.16.232.110, all of them have 101 as the inbound filter list.

```
router bgp 100
 neighbor external-peers peer-group
 neighbor external-peers route-map set-metric out
 neighbor external-peers filter-list 99 out
 neighbor external-peers filter-list 101 in
 neighbor 172.16.232.90 remote-as 200
 neighbor 172.16.232.90 peer-group external-peers
 neighbor 172.16.232.100 remote-as 300
 neighbor 172.16.232.100 peer-group external-peers
 neighbor 172.16.232.110 remote-as 400
 neighbor 172.16.232.110 peer-group external-peers
 neighbor 172.16.232.110 filter-list 400 in
```

Multiprotocol BGP Peer Group

In the following example, all members of the peer group are multicast-capable:

```
router bgp 100
neighbor 10.1.1.1 remote-as 1
neighbor 172.16.2.2 remote-as 2
address-family ipv4 multicast
 neighbor mygroup peer-group
 neighbor 10.1.1.1 peer-group mygroup
 neighbor 172.16.2.2 peer-group mygroup
 neighbor 10.1.1.1 activate
 neighbor 172.16.2.2 activate
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
clear ip bgp peer-group	Removes all the members of a BGP peer group.
show ip bgp peer-group	Displays information about BGP peer groups.

neighbor prefix-list

To prevent distribution of Border Gateway Protocol (BGP) neighbor information as specified in a prefix list, a Connectionless Network Service (CLNS) filter expression, or a CLNS filter set, use the **neighbor prefix-list** command in address family or router configuration mode. To remove a filter list, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **prefix-list** {*prefix-list-name* | *clns-filter-expr-name* | *clns-filter-set-name*} {**in** | **out**}

no neighbor {*ip-address* | *peer-group-name*} **prefix-list** {*prefix-list-name* | *clns-filter-expr-name* | *clns-filter-set-name*} {**in** | **out**}

Syntax Description

ip-address	IP address of neighbor.
peer-group-name	Name of a BGP peer group.
prefix-list-name	Name of a prefix list. This argument is used only under router configuration mode.
clns-filter-expr-name	Name of a CLNS filter expression. This argument is used only under network service access point (NSAP) address family configuration mode.
clns-filter-set-name	Name of a CLNS filter set. This argument is used only under NSAP address family configuration mode.
in	Filter list is applied to incoming advertisements from that neighbor.
out	Filter list is applied to outgoing advertisements to that neighbor.

Command Default

All external and advertised address prefixes are distributed to BGP neighbors.

Command Modes

Router configuration

Command History

Release	Modification
12.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(8)T	Under address family configuration mode, the *prefix-list-name* argument was amended to specify the name of a CLNS filter expression or a CLNS filter set.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Using prefix lists is one of three ways to filter BGP advertisements. You can also use AS-path filters, defined with the **ip as-path access-list** global configuration command and used in the **neighbor filter-list** command to filter BGP advertisements. The third way to filter BGP advertisements uses access or prefix lists with the **neighbor distribute-list** command.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group.

Use the **neighbor prefix-list** command in address family configuration mode to filter NSAP BGP advertisements.



Note Do not apply both a **neighbor distribute-list** and a **neighbor prefix-list** command to a neighbor in any given direction (inbound or outbound). These two commands are mutually exclusive, and only one command (**neighbor distribute-list** or **neighbor prefix-list**) can be applied to each inbound or outbound direction.

Examples

The following router configuration mode example applies the prefix list named *abc* to incoming advertisements from neighbor 10.23.4.1:

```
router bgp 65200
 network 192.168.1.2
 neighbor 10.23.4.1 prefix-list abc in
```

The following address family configuration mode example applies the prefix list named *abc* to incoming advertisements from neighbor 10.23.4.2:

```
router bgp 65001
address-family ipv4 unicast
 network 192.168.2.4
 neighbor 10.23.4.2 prefix-list abc in
```

The following router configuration mode example applies the prefix list named CustomerA to outgoing advertisements to neighbor 10.23.4.3:

```
router bgp 64800
 network 192.168.3.6
 neighbor 10.23.4.3 prefix-list CustomerA out
```

The following address family configuration mode example applies the CLNS filter list set named *default-prefix-only* to outbound advertisements to neighbor 10.1.2.1:

```
clns filter-set default-prefix-only deny 49...
clns filter-set default-prefix-only permit default
!
router bgp 65202
 address-family nsap
  neighbor 10.1.2.1 activate
  neighbor 10.1.2.1 default-originate
  neighbor 10.1.2.1 prefix-list default-prefix-only out
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enters the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.

address-family vpnv4	Enters the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
clear ip prefix-list	Resets the hit count of the prefix list entries.
clns filter-expr	Creates an entry in a CLNS filter expression.
clns filter-set	Creates an entry in a CLNS filter set.
ip as-path access-list	Defines a BGP-related access list.
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list description	Adds a text description of a prefix list.
ip prefix-list sequence-number	Enables the generation of sequence numbers for entries in a prefix list.
neighbor filter-list	Sets up a BGP filter.
show bgp nsap filter-list	Displays information about a filter list or filter list entries.
show ip bgp peer-group	Displays information about BGP peer groups.
show ip prefix-list	Displays information about a prefix list or prefix list entries.

neighbor remote-as

To add an entry to the BGP or multiprotocol BGP neighbor table, use the **neighbor remote-as** command in router configuration mode. To remove an entry from the table, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number* ...]

no neighbor {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number* ...]

Syntax Description

ip-address	IP address of the neighbor.
ipv6-address	IPv6 address of the neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
peer-group-name	Name of a BGP peer group.
autonomous-system-number	Number of an autonomous system to which the neighbor belongs in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command. When used with the **alternate-as** keyword, up to five autonomous system numbers may be entered.
alternate-as	(Optional) Specifies an alternate autonomous system in which a potential dynamic neighbor can be identified. Up to five autonomous system numbers may be entered when this keyword is specified.

Command Default

There are no BGP or multiprotocol BGP neighbor peers.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
11.0	The *peer-group-name* argument was added.

Release	Modification
11.1(20)CC	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(7)T	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were removed.
12.2(4)T	Support for the IPv6 address family was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. The **%** keyword was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH. The **alternate-as** keyword was added to support BGP dynamic neighbors.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

Specifying a neighbor with an autonomous system number that matches the autonomous system number specified in the **router bgp** global configuration command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered external.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only unicast address prefixes. To exchange other address prefix types, such as multicast and Virtual Private Network (VPN) Version 4, neighbors must also be activated in the appropriate address family configuration mode.

Use the **alternate-as** keyword introduced in Cisco IOS Release 12.2(33)SXH to specify up to five alternate autonomous systems in which a dynamic BGP neighbor may be identified. BGP dynamic neighbor support allows BGP peering to a group of remote neighbors that are defined by a range of IP addresses. BGP dynamic neighbors are configured using a range of IP addresses and BGP peer groups. After a subnet range is configured and associated with a BGP peer group using the **bgp listen** command and a TCP session is initiated for an IP address in the subnet range, a new BGP neighbor is dynamically created as a member of that group. The new BGP neighbor will inherit any configuration or templates for the group.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.



Note In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

To ensure a smooth transition, we recommend that all BGP speakers within an autonomous system that is identified using a 4-byte autonomous system number, be upgraded to support 4-byte autonomous system numbers.

Examples

The following example specifies that a router at the address 10.108.1.2 is an internal BGP (iBGP) neighbor in autonomous system number 65200:

```
router bgp 65200
 network 10.108.0.0
 neighbor 10.108.1.2 remote-as 65200
```

The following example specifies that a router at the IPv6 address 2001:0DB8:1:1000::72a is an external BGP (eBGP) neighbor in autonomous system number 65001:

```
router bgp 65300
 address-family ipv6 vrf site1
 neighbor 2001:0DB8:1:1000::72a remote-as 65001
```

The following example assigns a BGP router to autonomous system 65400, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 10.108.0.0 and 192.168.7.0 with the neighbor routers. The first router is a remote router in a different autonomous system from the router on which this configuration is entered (an eBGP neighbor); the second **neighbor remote-as** command shows an internal BGP neighbor (with the same autonomous

system number) at address 10.108.234.2; and the last **neighbor remote-as** command specifies a neighbor on a different network from the router on which this configuration is entered (also an eBGP neighbor).

```
router bgp 65400
 network 10.108.0.0
 network 192.168.7.0
 neighbor 10.108.200.1 remote-as 65200
 neighbor 10.108.234.2 remote-as 65400
 neighbor 172.29.64.19 remote-as 65300
```

The following example configures neighbor 10.108.1.1 in autonomous system 65001 to exchange only multicast routes:

```
router bgp 65001
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.31 1.2 remote-as 65001
 neighbor 172.16.2.2 remote-as 65002
 address-family ipv4 multicast
  neighbor 10.108.1.1 activate
  neighbor 172.31 1.2 activate
  neighbor 172.16.2.2 activate
  exit-address-family
```

The following example configures neighbor 10.108.1.1 in autonomous system 65001 to exchange only unicast routes:

```
router bgp 65001
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.31 1.2 remote-as 65001
 neighbor 172.16.2.2 remote-as 65002
```

The following example, configurable only in Cisco IOS Release 12.2(33)SXH and later releases, configures a subnet range of 192.168.0.0/16 and associates this listen range with a BGP peer group. Note that the listen range peer group that is configured for the BGP dynamic neighbor feature can be activated in the IPv4 address family using the **neighbor activate** command. After the initial configuration on Router 1, when Router 2 starts a BGP router session and adds Router 1 to its BGP neighbor table, a TCP session is initiated, and Router 1 creates a new BGP neighbor dynamically because the IP address of the new neighbor is within the listen range subnet.

Router 1

```
enable
configure terminal
router bgp 45000
 bgp log-neighbor-changes
 neighbor group192 peer-group
 bgp listen range 192.168.0.0/16 peer-group group192
 neighbor group192 remote-as 40000 alternate-as 50000
 address-family ipv4 unicast
 neighbor group192 activate
 end
```

Router 2

```
enable
configure terminal
router bgp 50000
 neighbor 192.168.3.1 remote-as 45000
 exit
```

If the **show ip bgp summary** command is now entered on Router 1, the output shows the dynamically created BGP neighbor, 192.168.3.2.

```
Router1# show ip bgp summary

BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1

BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

The following example configures a BGP process for autonomous system 65538 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asplain format. This example is supported only on Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or later releases.

```
router bgp 65538
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.3.2 remote-as 65550
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

The following example configures a BGP process for autonomous system 1.2 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asdot format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3, or a later release.

```
router bgp 1.2
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.3.2 remote-as 1.14
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
bgp listen	Associates a subnet range with a BGP peer group and activates the BGP dynamic neighbors feature.

neighbor peer-group	Creates a BGP peer group.
router bgp	Configures the BGP routing process.

neighbor remove-private-as

To remove private autonomous system numbers from tin outbound routing updates, use the **neighbor remove-private-as** command in router configuration, address family configuration, or peer-group template mode. To disable this function, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **remove-private-as** [**all** [**replace-as**]]

no neighbor {*ip-address* | *peer-group-name*} **remove-private-as**

Syntax Description

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
all	(Optional) Removes all private AS numbers from the AS path in outgoing updates.
replace-as	(Optional) As long as the **all** keyword is specified, the **replace-as** keyword causes all private AS numbers in the AS path to be replaced with the router's local AS number.

Command Default

No private AS numbers are removed from the AS path.

Command Modes

Router configuration
Address family configuration [Release 15.1(2)T and later]
Peer-group template [Release 15.1(2)T and later]

Command History

Release	Modification
10.3	This command was introduced.
11.0	The *peer-group-name* argument was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)T	This command was modified. The **all** keyword and the **replace-as** keyword were added.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

This command is available for external BGP (eBGP) neighbors only. The private AS values are 64512 to 65535.

When an update is passed to the external neighbor, if the AS path includes private AS numbers, the software will drop the private AS numbers.

Behavior Before Release 15.1(2)T

- If the AS path includes both private and public AS numbers, the software considers this to be a configuration error and does not remove the private AS numbers.
- If the AS path contains the AS number of the eBGP neighbor, the private AS numbers are not removed.
- If this command is used with confederation, it will work as long as the private AS numbers follow the confederation portion of the AS path.

Behavior in Release 15.1(2)T and Later

- The **neighbor remove-private-as** command removes private AS numbers from the AS path even if the path contains both public and private ASNs.
- The **neighbor remove-private-as** command removes private AS numbers even if the AS path contains only private AS numbers. There is no likelihood of a 0-length AS path because this command can be applied to eBGP peers only, in which case the AS number of the local router is appended to the AS path.
- The **neighbor remove-private-as** command removes private AS numbers even if the private ASNs appear before the Confederation segments in the AS path.
- Upon removing private AS numbers from the AS path, the path length of prefixes being sent out will decrease. Because the AS path length is a key element of BGP best path selection, it might be necessary to retain the path length. The **replace-as** keyword ensures that the path length is retained by replacing all removed AS numbers with the local router's AS number.
- The feature can be applied to neighbors per address family. Therefore, you can apply the feature to a neighbor in one address family and not in another, affecting update messages on the outbound side for only the address family for which the feature is configured.

Examples

The following example shows a configuration that removes the private AS number from the updates sent to 172.16.2.33. The result is that the AS path for the paths advertised by 10.108.1.1 through AS 100 will contain only "100" (as seen by autonomous system 2051).

```
router bgp 100
 neighbor 10.108.1.1 description peer with private-as
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.16.2.33 description eBGP peer
 neighbor 172.16.2.33 remote-as 2051
 neighbor 172.16.2.33 remove-private-as

Router-in-AS100# show ip bgp 10.0.0.0

BGP routing table entry for 10.0.0.0/8, version 15
Paths: (1 available, best #1)
  Advertised to non peer-group peers:
    172.16.2.33
  65001
    10.108.1.1 from 10.108.1.1
      Origin IGP, metric 0, localpref 100, valid, external, best

Router-in-AS2501# show ip bgp 10.0.0.0

BGP routing table entry for 10.0.0.0/8, version 3
Paths: (1 available, best #1)
  Not advertised to any peer
  2
```

```
    172.16.2.32 from 172.16.2.32
      Origin IGP, metric 0, localpref 100, valid, external, best
```

The following is an example of removing and replacing private ASNs using Cisco IOS Release 15.1(2)T or later. In this example, when Router A sends prefixes to the peer 172.30.0.7, all private ASNs in the AS path are replaced with the router's own ASN, which is 100.

Router A

```
router bgp 100
 bgp log-neighbor-changes
 neighbor 172.16.101.1 remote-as 1001
 neighbor 172.16.101.1 update-source Loopback0
 neighbor 172.30.0.7 remote-as 200
 neighbor 172.30.0.7 remove-private-as all replace-as
 no auto-summary
```

Router A receives 1.1.1.1 from peer 172.16.101.1, which has some private ASNs (65200, 65201, and 65201) in the AS path list, as shown in the following output:

```
RouterA# show ip bgp 1.1.1.1

BGP routing table entry for 1.1.1.1/32, version 2
Paths: (1 available, best #1, table default)
   Advertised to update-groups:
      1          2
   1001 65200 65201 65201 1002 1003 1003
     172.16.101.1 from 172.16.101.1 (172.16.101.1)
       Origin IGP, localpref 100, valid, external, best RouterA#
```

Because Router A is configured with **neighbor 172.30.0.7 remove-private-as all replace-as**, Router A sends prefix 1.1.1.1 with all private ASNs replaced with 100:

Router B

```
RouterB# show ip bgp 1.1.1.1

BGP routing table entry for 1.1.1.1/32, version 3
Paths: (1 available, best #1, table default)
   Not advertised to any peer
   100 1001 100 100 100 1002 1003 1003
     172.30.0.6 from 172.30.0.6 (192.168.1.2)
       Origin IGP, localpref 100, valid, external, best RouterB#
```

Router B

```
router bgp 200
 bgp log-neighbor-changes
 neighbor 172.30.0.6 remote-as 100
 no auto-summary
```

Related Commands

Command	Description
neighbor remote-as	Allows entries to the BGP neighbor table.
show ip bgp neighbor	Displays entries in the BGP routing table.
show ip bgp update-group	Displays entries in the BGP routing table.

neighbor route-map

To apply a route map to incoming or outgoing routes, use the **neighbor route-map** command in address family or router configuration mode. To remove a route map, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name* | *ipv6-address* [**%**]} **route-map** *map-name* {**in** | **out**}

no neighbor {*ip-address* | *peer-group-name* | *ipv6-address* [**%**]} **route-map** *map-name* {**in** | **out**}

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP or multiprotocol BGP peer group.
ipv6-address	IPv6 address of the neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
map-name	Name of a route map.
in	Applies route map to incoming routes.
out	Applies route map to outgoing routes.

Command Default

No route maps are applied to a peer.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(4)T	Support for IPv6 was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **%** keyword was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

When specified in address family configuration mode, this command applies a route map to that particular address family only. When specified in router configuration mode, this command applies a route map to IPv4 or IPv6 unicast routes only.

If an outbound route map is specified, it is proper behavior to only advertise routes that match at least one section of the route map.

If you specify a BGP or multiprotocol BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

Examples

The following router configuration mode example applies a route map named internal-map to a BGP incoming route from 172.16.70.24:

```
router bgp 5
 neighbor 172.16.70.24 route-map internal-map in

route-map internal-map
 match as-path 1
 set local-preference 100
```

The following address family configuration mode example applies a route map named internal-map to a multiprotocol BGP incoming route from 172.16.70.24:

```
router bgp 5
address-family ipv4 multicast
 neighbor 172.16.70.24 route-map internal-map in

route-map internal-map
 match as-path 1
 set local-preference 100
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions that use standard VPNv6 address prefixes.
neighbor remote-as	Creates a BGP peer group.

neighbor route-reflector-client

To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the **neighbor route-reflector-client** command in address family or router configuration mode. To indicate that the neighbor is not a client, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**

Syntax Description

ip-address	IP address of the BGP neighbor being identified as a client.
ipv6-address	IPv6 address of the BGP neighbor being identified as a client.
peer-group-name	Name of a BGP peer group.

Command Default

There is no route reflector in the autonomous system.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
11.1	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The *ipv6-address* and *peer-group-name* arguments were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was updated. It was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

By default, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop. When all the clients are disabled, the local router is no longer a route reflector.

If you use route reflectors, all iBGP speakers need not be fully meshed. In the route reflector model, an Interior BGP peer is configured to be a *route reflector* responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.

Use the **neighbor route-reflector-client** command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.

The **bgp client-to-client reflection** command controls client-to-client reflection.

Examples

In the following router configuration mode example, the local router is a route reflector. It passes learned iBGP routes to the neighbor at 172.16.70.24.

```
router bgp 5
 neighbor 172.16.70.24 route-reflector-client
```

In the following address family configuration mode example, the local router is a route reflector. It passes learned iBGP routes to the neighbor at 172.16.70.24.

```
router bgp 5
address-family ipv4 unicast
 neighbor 172.16.70.24 route-reflector-client
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard VPNv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard VPNv6 address prefixes.
bgp client-to-client reflection	Restores route reflection from a BGP route reflector to clients.
bgp cluster-id	Configures the cluster ID if the BGP cluster has more than one route reflector.
neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
show bgp ipv6	Displays entries in the IPv6 BGP routing table.
show ip bgp	Displays entries in the BGP routing table.

neighbor send-community

To specify that a communities attribute should be sent to a BGP neighbor, use the **neighbor send-community** command in address family or router configuration mode. To remove the entry, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community**

Syntax Description

ip-address	IP address of the neighbor.
ipv6-address	IPv6 address of the neighbor.
peer-group-name	Name of a BGP peer group.
both	(Optional) Specifies that both standard and extended communities will be sent.
standard	(Optional) Specifies that only standard communities will be sent.
extended	(Optional) Specifies that only extended communities will be sent.

Command Default

No communities attribute is sent to any neighbor.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
10.3	This command was introduced.
11.0	The *peer-group-name* argument was added.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The *ipv6-address* argument was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

In the following router configuration mode example, the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 109
 neighbor 172.16.70.23 send-community
```

In the following address family configuration mode example, the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 109
address-family ipv4 multicast
 neighbor 172.16.70.23 send-community
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.
match community	Matches a BGP community.
neighbor remote-as	Creates a BGP peer group.
set community	Sets the BGP communities attribute.

neighbor shutdown

To disable a neighbor or peer group, use the **neighbor shutdown** command in router configuration mode. To reenable the neighbor or peer group, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **shutdown**

no neighbor {*ip-address* | *peer-group-name*} **shutdown**

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.

Defaults

No change is made to the status of any BGP neighbor or peer group.

Command Modes

Router configuration

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **neighbor shutdown** command terminates any active session for the specified neighbor or peer group and removes all associated routing information. In the case of a peer group, a large number of peering sessions could be terminated suddenly.

To display a summary of BGP neighbors and peer group connections, use the **show ip bgp summary** command. Those neighbors with an Idle status and the Admin entry have been disabled by the **neighbor shutdown** command.

"State/PfxRcd" shows the current state of the BGP session or the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the **neighbor maximum-prefix** command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is idle.

Examples

The following example disables any active session for the neighbor 172.16.70.23:

```
neighbor 172.16.70.23 shutdown
```

The following example disables all peering sessions for the peer group named internal:

```
neighbor internal shutdown
```

Related Commands

Command	Description
neighbor maximum-prefix	Controls how many prefixes can be received from a neighbor.
show ip bgp summary	Displays the status of all BGP connections.

neighbor slow-peer detection

To specify a threshold time that dynamically determines a slow peer, use the **neighbor slow-peer detection** command in address-family configuration mode. To remove dynamic slow peer detection for a neighbor, use the **no** form of this command.

neighbor {*neighbor-address* | *peer-group-name*} **slow-peer detection** [**disable** | **threshold** *seconds*]

no neighbor {*neighbor-address* | *peer-group-name*} **slow-peer detection**

Syntax Description

neighbor-address	IP address of a BGP neighbor whose update messages are being compared to the current time to determine slowness.
peer-group-name	Peer group name of the bgp neighbors whose update messages are being compared to the current time to determine slowness.
disable	(Optional) Disables slow peer detection for the specified neighbor even if slow peer detection is enabled at the global, address-family level.
threshold *seconds*	(Optional) Threshold time in seconds that the timestamp of the oldest message in a peers queue can be lagging behind the current time before the peer is determined to be a slow peer. The range is from 120 to 3600; the default is 300.

Command Default

No neighbor is configured as a dynamic slow peer.

Command Modes

Address-family configuration (config-router-af)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

Update messages are timestamped when they are formatted. The timestamp of the oldest message in a peers queue is compared to the current time to determine if the peer is lagging more than the configured number of seconds. When a peer is dynamically detected to be a slow peer, the system will send a syslog message. The peer will be marked as recovered and another syslog message will be generated only after the peer's update group converges.

You can use this command alone just to detect a slow peer, or you can use this command with the **neighbor slow-peer split-update-group dynamic** command to move the peer to a slow update group.

Note The **neighbor slow-peer detection** command performs the same function as the **bgp slow-peer detection** command (at the address-family level). The **neighbor slow-peer detection** command overrides the global, address-family level command. If the **neighbor slow-peer detection** command is unconfigured or if **no neighbor slow-peer detection** is configured, the system will inherit the global, address-family level configuration.

Note The **slow-peer detection** command performs the same function through a peer policy template.

Examples

The following example sets a threshold of 400 seconds for the BGP peer at 10.4.4.4. Once the current time is more than 400 seconds later than the timestamp on the oldest message in that peers queue, the peer is determined to be a slow peer.

```
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 10.4.4.4 slow-peer detection threshold 400
Router(config-router-af)# neighbor 10.4.4.4 slow-peer split-update-group dynamic
```

In the following example, both neighbors 4.4.4.4 and 6.6.6.6 have slow peer detection enabled for them due to the global command **bgp slow-peer detection**:

```
Router(config)# router bgp 100
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 4.4.4.4 remote-as 100
Router(config-router)# neighbor 6.6.6.6 remote-as 100
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp slow-peer detection
Router(config-router-af)# neighbor 4.4.4.4 activate
Router(config-router-af)# neighbor 6.6.6.6 activate
Router(config-router-af)# no auto-summary
Router(config-router-af)# exit-address-family
Router(config-router)#
```

To disable slow peer detection for a particular peer, use the **disable** keyword. The following example disables slow peer detection for the neighbor 4.4.4.4:

```
Router(config)# router bgp 100
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 4.4.4.4 remote-as 100
Router(config-router)# neighbor 6.6.6.6 remote-as 100
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp slow-peer detection
Router(config-router-af)# neighbor 4.4.4.4 activate
Router(config-router-af)# neighbor 4.4.4.4 slow-peer detection disable
Router(config-router-af)# neighbor 6.6.6.6 activate
Router(config-router-af)# no auto-summary
Router(config-router-af)# exit-address-family
Router(config-router)#
```

Related Commands

Command	Description
bgp slow-peer detection	Specifies a threshold time that dynamically determines a slow peer at the global, address family level.
clear ip bgp slow	Moves dynamically configured slow peers back to their original update groups.
neighbor slow-peer split-update-group dynamic	Moves a dynamically detected slow peer to a slow update group.

neighbor slow-peer split-update-group dynamic

To move a dynamically detected slow peer to a slow update group, use the **neighbor slow-peer split-update-group dynamic** command in address-family configuration mode. To cancel this method of moving dynamically detected slow peers to a slow update group, use the **no** form of this command.

neighbor {*neighbor-address* | *peer-group-name*} **slow-peer split-update-group dynamic** [**permanent** | **disable**]

no neighbor {*neighbor-address* | *peer-group-name*} **slow-peer split-update-group dynamic**

Syntax Description

neighbor-address	IP address of a BGP neighbor peer that is moved to the slow peer group if dynamically determined to be slow.
peer-group-name	Peer group name of the BGP neighbor peers that are moved to the slow peer group if dynamically determined to be slow.
permanent	(Optional) Specifies that after the slow peer becomes a regular peer (converges), it is not moved back to its original update group automatically. The network administrator can use one of the **clear** commands to move the peer to its original update group.
disable	(Optional) Disables slow peer protection for the specified neighbor even if slow peer protection is enabled at the global, address-family level.

Command Default

No dynamically detected slow peer is moved to a slow peer update group.

Command Modes

Address-family configuration (config-router-af)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

When a peer is dynamically detected to be a slow peer, the slow peer is moved to a slow update group. If a *static* slow peer update group exists, the dynamic slow peer is moved to the static slow peer update group; otherwise, a new slow peer updated group is created and the peer is moved to that group.

- If the **permanent** keyword is not configured, the slow peer will be moved back to its regular original update group after it becomes a regular peer (converges).
- If the **permanent** keyword is configured, the peer is not automatically moved to its original update group. You can use one of the **clear** commands to move the peer back to its original update group.

If no slow peer detection is configured, the detection will be done at the default threshold of 300 seconds.

The **neighbor slow-peer-split-update-group dynamic** command will override the global configuration. However, if the **no neighbor slow-peer-split-update-group dynamic** command is configured, then the peers will inherit the global address family configuration specified by the **bgp slow-peer detection** command.

Examples

In the following example, the timestamp of the oldest message in a peers queue is compared to the current time to determine if the peer is lagging more than 360 seconds. If it is, the neighbor who sent the message is determined to be a slow peer, and is put in the slow peer update group. Because the **permanent** keyword is not configured, the slow peer will be moved back to its regular original update group after it becomes a regular peer (converges).

```
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 10.4.4.4 slow-peer detection threshold 360
Router(config-router-af)# neighbor 10.4.4.4 slow-peer split-update-group dynamic
```

In the following example, both neighbors 4.4.4.4 and 6.6.6.6 have slow peer protection enabled for them due to the global command **bgp slow-peer split-update-group dynamic**:

```
Router(config)# router bgp 100
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 4.4.4.4 remote-as 100
Router(config-router)# neighbor 6.6.6.6 remote-as 100
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp slow-peer split-update-group dynamic
Router(config-router-af)# neighbor 4.4.4.4 activate
Router(config-router-af)# neighbor 6.6.6.6 activate
Router(config-router-af)# no auto-summary
Router(config-router-af)# exit-address-family
Router(config-router)#
```

To disable slow peer protection for a particular peer, use the **disable** keyword. The following example disables slow peer protection for the neighbor 4.4.4.4:

```
Router(config)# router bgp 100
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 4.4.4.4 remote-as 100
Router(config-router)# neighbor 6.6.6.6 remote-as 100
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp slow-peer detection
Router(config-router-af)# neighbor 4.4.4.4 activate
Router(config-router-af)# neighbor 4.4.4.4 slow-peer split-update-group dynamic disable
Router(config-router-af)# neighbor 6.6.6.6 activate
Router(config-router-af)# no auto-summary
Router(config-router-af)# exit-address-family
Router(config-router)#
```

Related Commands

Command	Description
clear ip bgp slow	Moves dynamically configured slow peers back to their original update groups.
neighbor slow-peer detection	Specifies a threshold time that dynamically determines a slow peer in neighbor address family configuration mode.

neighbor slow-peer split-update-group static

To mark a BGP neighbor as a slow peer and move it to a slow update group, use the **neighbor slow-peer split-update-group static** command in address-family configuration mode. To unmark the slow peer and return it to its original update group, use the **no** form of this command.

neighbor {*neighbor-address* | *peer-group-name*} **slow-peer split-update-group static**

no neighbor {*neighbor-address* | *peer-group-name*} **slow-peer split-update-group static**

Syntax Description

neighbor-address	IP address of a BGP neighbor peer that is marked as slow and moved to a slow peer group.
peer-group-name	Peer group name of the BGP neighbor peers that are marked as slow and moved to a slow peer group.

Command Default

No peer is statically marked as slow and moved to a slow peer update group, unless through a peer policy template or configured at neighbor or peer group.

Command Modes

Address-family configuration (config-router-af)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

Configure a static slow peer when the peer is known to be slow (perhaps due to a slow link or low processing power).

The **slow-peer split-update-group static** command performs the same function through a peer policy template.

Examples

In the following example, the neighbor with the specified IP address is marked as a slow peer and is moved to a slow update group.

```
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 172.20.2.2 slow-peer split-update-group static
```

Related Commands

Command	Description
slow-peer split-update-group static	Marks a BGP neighbor as a static slow peer and moves it to a slow update group.

neighbor soft-reconfiguration

To configure the Cisco IOS software to start storing updates, use the **neighbor soft-reconfiguration** command in router configuration mode. To not store received updates, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **soft-reconfiguration inbound**

no neighbor {*ip-address* | *peer-group-name*} **soft-reconfiguration inbound**

Syntax Description

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
inbound	Indicates that the update to be stored is an incoming update.

Defaults

Soft reconfiguration is not enabled.

Command Modes

Router configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Entering this command starts the storage of updates, which is required to do inbound soft reconfiguration. Outbound BGP soft reconfiguration does not require inbound soft reconfiguration to be enabled.

To use soft reconfiguration, or soft reset, without preconfiguration, both BGP peers must support the soft route refresh capability, which is advertised in the open message sent when the peers establish a TCP session. Routers running Cisco IOS software releases prior to Release 12.1 do not support the route refresh capability and must clear the BGP session using the **neighbor soft-reconfiguration** command. Clearing the BGP session using the **neighbor soft-reconfiguration** command has a negative effect on network operations and should only be used as a last resort. Routers running Cisco IOS software Release 12.1 or later releases support the route refresh capability and dynamic soft resets, and can use the **clear ip bgp** {***** | *address* | *peer-group name*} **in** command to clear the BGP session.

To determine whether a BGP router supports this capability, use the **show ip bgp neighbors** command. If a router supports the route refresh capability, the following message is displayed:

```
Received route refresh capability from peer.
```

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

The following example enables inbound soft reconfiguration for the neighbor 10.108.1.1. All the updates received from this neighbor will be stored unmodified, regardless of the inbound policy. When inbound soft reconfiguration is done later, the stored information will be used to generate a new set of inbound updates.

```
router bgp 100
 neighbor 10.108.1.1 remote-as 200
 neighbor 10.108.1.1 soft-reconfiguration inbound
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection using BGP soft reconfiguration.
neighbor remote-as	Creates a BGP peer group.
show ip bgp neighbors	Display information about the TCP and BGP connections to neighbors.

neighbor soo

To set the site-of-origin (SoO) value for a Border Gateway Protocol (BGP) neighbor or peer group, use the **neighbor soo** command in address family IPv4 VRF configuration mode. To remove the SoO value for a BGP neighbor or peer group, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **soo** *extended-community-value*

no neighbor {*ip-address* | *peer-group-name*} **soo**

Syntax Description

ip-address	IP address of a neighboring router.
peer-group-name	Name of a BGP peer group.
extended-community-value	Specifies the VPN extended community value. The value takes one of the following formats: • A 16-bit autonomous system number, a colon, and a 32-bit number, for example: 45000:3 • A 32-bit IP address, a colon, and a 16-bit number, for example: 192.168.10.2:51 In Cisco IOS Release 12.4(24)T, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. In Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. For more details about autonomous system number formats, see the **router bgp** command.

Command Default

No SoO value is set for a BGP neighbor or peer group.

Command Modes

Address family IPv4 VRF configuration (config-router-af)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.

Release	Modification
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

Use this command to set the SoO value for a BGP neighbor. The SoO value is set under address family IPv4 VRF configuration mode either directly for a neighbor or for a BGP peer group.

The SoO extended community is a BGP extended community attribute that is used to identify routes that have originated from a site so that the readvertisement of that prefix back to the source site can be prevented. The SoO extended community uniquely identifies the site from which a router has learned a route. BGP can use the SoO value associated with a route to prevent routing loops.

In releases prior to Cisco IOS Release 12.4(11)T, 12.2(33)SRB, and 12.2(33)SB, the SoO extended community attribute is configured using an inbound route map that sets the SoO value during the update process. The introduction of the **neighbor soo** and **soo** commands simplifies the SoO value configuration.

Note A BGP neighbor or peer policy template-based SoO configuration takes precedence over an SoO value configured in an inbound route map.

In Cisco IOS Release 12.4(24)T, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

In Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

Examples

The following example shows how to configure an SoO value for a BGP neighbor. Under address family IPv4 VRF, a neighbor is identified and an SoO value is configured for the neighbor.

```
router bgp 45000
 address-family ipv4 vrf VRF_SOO
  neighbor 192.168.1.2 remote-as 40000
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.2 soo 45000:40
  end
```

The following example shows how to configure an SoO value for a BGP peer group. Under address family IPv4 VRF, a BGP peer group is configured, an SoO value is configured for the peer group, a neighbor is identified, and the neighbor is configured as a member of the peer group.

```
router bgp 45000
 address-family ipv4 vrf VRF_SOO
  neighbor SOO_GROUP peer-group
  neighbor SOO_GROUP soo 45000:65
  neighbor 192.168.1.2 remote-as 40000
```

```
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.2 peer-group SOO_GROUP
  end
```

The following example shows how to configure an SoO value for a BGP neighbor using 4-byte autonomous system numbers. Under address family IPv4 VRF, a neighbor is identified and an SoO value of 1.2:1 is configured for the neighbor. This example requires Cisco IOS Release 12.4(24)T, Cisco IOS XE Release 2.4, or a later release.

```
router bgp 1.2
 address-family ipv4 vrf site1
  neighbor 192.168.1.2 remote-as 1.14
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.2 soo 1.2:1
  end
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enters address family configuration mode to configure a routing session using standard IP Version 4 address prefixes.
router bgp	Configures the BGP routing process.
soo	Sets the SoO value for a BGP peer policy template.

neighbor timers

To set the timers for a specific BGP peer or peer group, use the **neighbor timers** command in address family or router configuration mode. To clear the timers for a specific BGP peer or peer group, use the **no** form of this command.

neighbor [*ip-address* | *peer-group-name*] **timers** *keepalive holdtime* [*min-holdtime*]

no neighbor [*ip-address* | *peer-group-name*] **timers**

Syntax Description

ip-address	(Optional) A BGP peer or peer group IP address.
peer-group-name	(Optional) Name of the BGP peer group.
keepalive	Frequency (in seconds) with which the Cisco IOS software sends *keepalive* messages to its peer. The default is 60 seconds.The range is from 0 to 65535.
holdtime	Interval (in seconds) after not receiving a *keepalive* message that the software declares a peer dead. The default is 180 seconds. The range is from 0 to 65535.
min-holdtime	(Optional) Interval (in seconds) specifying the minimum acceptable hold-time from a BGP neighbor. The minimum acceptable hold-time must be less than, or equal to, the interval specified in the *holdtime* argument. The range is from 0 to 65535.

Defaults

keepalive: 60 seconds
holdtime: 180 seconds

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0	This command was introduced.
12.0(26)S	The *min-holdtime* argument was added.
12.3(7)T	The *min-holdtime* argument was added.
12.2(22)S	The *min-holdtime* argument was added.
12.2(27)SBC	The *min-holdtime* argument was added and this command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	The *min-holdtime* argument was added and this command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	The *min-holdtime* argument was added and this command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The timers configured for a specific neighbor or peer group override the timers configured for all BGP neighbors using the **timers bgp** command.

When configuring the *holdtime* argument for a value of less than twenty seconds, the following warning is displayed:

```
% Warning: A hold time of less than 20 seconds increases the chances of peer flapping
```

If the minimum acceptable hold-time interval is greater than the specified hold-time, a notification is displayed:

```
% Minimum acceptable hold time should be less than or equal to the configured hold time
```



Note When the minimum acceptable hold-time is configured on a BGP router, a remote BGP peer session is established only if the remote peer is advertising a hold-time that is equal to, or greater than, the minimum acceptable hold-time interval. If the minimum acceptable hold-time interval is greater than the configured hold-time, the next time the remote session tries to establish, it will fail and the local router will send a notification stating “unacceptable hold time.”

Examples

The following example changes the keepalive timer to 70 seconds and the hold-time timer to 210 seconds for the BGP peer 192.168.47.0:

```
router bgp 109
 neighbor 192.168.47.0 timers 70 210
```

The following example changes the keepalive timer to 70 seconds, the hold-time timer to 130 seconds, and the minimum hold-time interval to 100 seconds for the BGP peer 192.168.1.2:

```
router bgp 45000
 neighbor 192.168.1.2 timers 70 130 100
```

neighbor transport

To enable a TCP transport session option for a Border Gateway Protocol (BGP) session, use the **neighbor transport** command in router or address family configuration mode. To disable a TCP transport session option for a BGP session, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **transport** {**connection-mode** {**active** | **passive**} | **path-mtu-discovery** | **multi-session** | **single-session**}

no neighbor {*ip-address* | *peer-group-name*} **transport** {**connection-mode** | **path-mtu-discovery** | **multi-session** | **single-session**}

Syntax Description

ip-address	IP address of the BGP neighbor.
peer-group-name	Name of a BGP peer group.
connection-mode	Specifies the type of connection.
active	Specifies an active connection.
passive	Specifies a passive connection.
path-mtu-discovery	Enables TCP transport path maximum transmission unit (MTU) discovery. TCP path MTU discovery is enabled by default.
multi-session	Enables a separate TCP transport session for each address family.
single-session	Enables all address families to use a single TCP transport session.

Command Default

If this command is not configured, TCP path MTU discovery is enabled by default, but no other TCP transport session options are enabled.

Command Modes

Router configuration (config-router)
Address family configuration (config-router-af)

Command History

Release	Modification
12.4	This command was introduced.
12.2(33)SRA	The **path-mtu-discovery** keyword was added.
12.2(33)SRB	The **multi-session** and **single-session** keywords were added.
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	The **path-mtu-discovery** keyword was added.

Usage Guidelines

This command is used to specify various transport options. An active or passive transport connection can be specified for a BGP session. TCP transport path MTU discovery can be enabled to allow a BGP session to take advantage of larger MTU links. Use the **show ip bgp neighbors** command to determine whether TCP path MTU discovery is enabled.

In Cisco IOS Release 12.2(33)SRB and later releases, options can be specified for the transport of address family traffic using a single TCP session or to enable a separate TCP session for each address family. Multiple TCP sessions are used to support Multi-Topology Routing (MTR), and the single session option is available for backwards compatibility for non-MTR configurations and for scalability purposes.

Examples

The following example shows how to configure the TCP transport connection to be active for a single internal BGP (iBGP) neighbor:

```
router bgp 45000
 neighbor 172.16.1.2 remote-as 45000
 neighbor 172.16.1.2 activate
 neighbor 172.16.1.2 transport connection-mode active
 end
```

The following example shows how to configure the TCP transport connection to be passive for a single external BGP (eBGP) neighbor:

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 activate
 neighbor 192.168.1.2 transport connection-mode passive
 end
```

The following example shows how to disable TCP path MTU discovery for a single BGP neighbor:

```
router bgp 45000
 neighbor 172.16.1.2 remote-as 45000
 neighbor 172.16.1.2 activate
 no neighbor 172.16.1.2 transport path-mtu-discovery
 end
```

The following example shows how to reenable TCP path MTU discovery for a single BGP neighbor, if TCP path MTU discovery is disabled:

```
router bgp 45000
 neighbor 172.16.1.2 remote-as 45000
 neighbor 172.16.1.2 activate
 neighbor 172.16.1.2 transport path-mtu-discovery
 end
```

The following example shows how to enable a separate TCP session for each address family for an MTR topology configuration:

```
router bgp 45000
 scope global
  neighbor 172.16.1.2 remote-as 45000
  neighbor 172.16.1.2 transport multi-session
  address-family ipv4
   topology VIDEO
   bgp tid 100
   neighbor 172.16.1.2 activate
   end
```

Related Commands

Command	Description
bgp tid	Configures BGP to accept routes with a specified topology ID.
bgp transport	Enables transport session parameters globally for all BGP neighbor sessions.

Command	Description
scope	Defines the scope for a BGP routing session and enters router scope configuration mode.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.
topology (BGP)	Configures a process to route IP traffic under the specified topology instance.

neighbor ttl-security

To secure a Border Gateway Protocol (BGP) peering session and to configure the maximum number of hops that separate two external BGP (eBGP) peers, use the **neighbor ttl-security** command in address-family or router configuration mode. To disable this feature, use the **no** form of this command.

neighbor *neighbor-address* **ttl-security hops** *hop-count*

no neighbor *neighbor-address* **ttl-security hops** *hop-count*

Syntax Description

neighbor-address	IP address of the neighbor.
hops *hop-count*	Number of hops that separate the eBGP peers. The TTL value is calculated by the router from the configured *hop-count* argument. The value for the *hop-count* argument is a number between 1 and 254.

Defaults

No default behavior or values

Command Modes

Address-family configuration
Router configuration

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

The **neighbor ttl-security** command provides a lightweight security mechanism to protect BGP peering sessions from CPU utilization-based attacks. These types of attacks are typically brute force Denial of Service (DoS) attacks that attempt to disable the network by flooding the network with IP packets that contain forged source and destination IP addresses in the packet headers.

This feature leverages designed behavior of IP packets by accepting only IP packets with a TTL count that is equal to or greater than the locally configured value. Accurately forging the TTL count in an IP packet is generally considered to be impossible. Accurately forging a packet to match the TTL count from a trusted peer is not possible without internal access to the source or destination network.

This feature should be configured on each participating router. It secures the BGP session in the incoming direction only and has no effect on outgoing IP packets or the remote router. When this feature is enabled, BGP will establish or maintain a session only if the TTL value in the IP packet header is equal to or greater than the TTL value configured for the peering session. This feature has no effect on the BGP peering session, and the peering session can still expire if keepalive packets are not received. If the TTL

value in a received packet is less than the locally configured value, the packet is silently discarded and no Internet Control Message Protocol (ICMP) message is generated. This is designed behavior; a response to a forged packet is not necessary.

To maximize the effectiveness of this feature, the *hop-count* value should be strictly configured to match the number of hops between the local and external network. However, you should also take path variation into account when configuring this feature for a multihop peering session.

The following restrictions apply to the configuration of this command:

- This feature is not supported for internal BGP (iBGP) peers or iBGP peer groups.
- The **neighbor ttl-security** command cannot be configured for a peer that is already configured with the **neighbor ebgp-multihop** command. The configuration of these commands is mutually exclusive, and only one of these commands is needed to enable a multihop eBGP peering session. An error message will be displayed in the console if you attempt to configure both commands for the same peering session.
- The effectiveness of this feature is reduced in large-diameter multihop peerings. In the event of a CPU utilization-based attack against a BGP router that is configured for large-diameter peering, you may still need to shut down the affected peering sessions to handle the attack.
- This feature is not effective against attacks from a peer that has been compromised inside of your network. This restriction also includes peers that are on the network segment between the source and destination network.

Examples

The following example sets the hop count to 2 for a directly connected neighbor. Because the *hop-count* argument is set to 2, BGP will accept only IP packets with a TTL count in the header that is equal to or greater than 253. If a packet is received with any other TTL value in the IP packet header, the packet will be silently discarded.

```
neighbor 10.0.0.1 ttl-security hops 2
```

Related Commands

Command	Description
neighbor ebgp-multihop	Accepts or initiates BGP connections to external peers residing on networks that are not directly connected.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

neighbor unsuppress-map

To selectively advertise routes previously suppressed by the **aggregate-address** command, use the **neighbor unsuppress-map** command in address family or router configuration mode. To restore the system to the default condition, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **unsuppress-map** *route-map-name*

no neighbor {*ip-address* | *peer-group-name*} **unsuppress-map** *route-map-name*

Syntax Description

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
route-map-name	Name of a route map.

Command Default

No routes are unsuppressed.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use of the **neighbor unsuppress-map** command allows specified suppressed routes to be advertised.

Examples

The following BGP router configuration shows that routes specified by a route map named map1 are suppressed:

```
access-list 3 deny 172.16.16.6
access-list 3 permit any
route-map map1 permit 10
match ip address 3
!
router bgp 65000
network 172.16.0.0
neighbor 192.168.1.2 remote-as 40000
aggregate-address 172.0.0.0 255.0.0.0 suppress-map map1
neighbor 192.168.1.2 unsuppress-map map1
neighbor 192.168.1.2 activate
```

The following example shows the routes specified by internal-map being unsuppressed for neighbor 172.16.16.6:

```
router bgp 100
address-family ipv4 multicast
 network 172.16.0.0
 neighbor 172.16.16.6 unsuppress-map internal-map
```

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 routing in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
aggregate-address	Creates an aggregate entry in a BGP routing table.
neighbor route-map	Applies a route map to inbound or outbound routes.

neighbor update-source

To have the Cisco IOS software allow Border Gateway Protocol (BGP) sessions to use any operational interface for TCP connections, use the **neighbor update-source** command in router configuration mode. To restore the interface assignment to the closest interface, which is called the best local address, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **update-source** *interface-type interface-number*

no neighbor {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **update-source** *interface-type interface-number*

Syntax Description

ip-address	IPv4 address of the BGP-speaking neighbor.
ipv6-address	IPv6 address of the BGP-speaking neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
peer-group-name	Name of a BGP peer group.
interface-type	Interface type.
interface-number	Interface number.

Command Default

Best local address

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.2(4)T	The *ipv6-address* argument was added.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **%** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

This command can work in conjunction with the loopback interface feature described in the "Interface Configuration Overview" chapter of the *Cisco IOS Interface and Hardware Component Configuration Guide*.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

The **neighbor update-source** command must be used to enable IPv6 link-local peering for internal or external BGP sessions.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces and for these link-local IPv6 addresses you must specify the interface they are on. The syntax becomes <IPv6 local-link address>%<interface name>, for example, FE80::1%Ethernet1/0. Note that the interface type and number must not contain any spaces, and be used in full-length form because name shortening is not supported in this situation. The % keyword and subsequent interface syntax is not used for non-link-local IPv6 addresses.

Examples

The following example sources BGP TCP connections for the specified neighbor with the IP address of the loopback interface rather than the best local address:

```
router bgp 65000
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 110
 neighbor 172.16.2.3 update-source Loopback0
```

The following example sources IPv6 BGP TCP connections for the specified neighbor in autonomous system 65000 with the global IPv6 address of loopback interface 0 and the specified neighbor in autonomous system 65400 with the link-local IPv6 address of Fast Ethernet interface 0/0. Note that the link-local IPv6 address of FE80::2 is on Ethernet interface 1/0.

```
router bgp 65000
 neighbor 3ffe::3 remote-as 65000
 neighbor 3ffe::3 update-source Loopback0
 neighbor fe80::2%Ethernet1/0 remote-as 65400
 neighbor fe80::2%Ethernet1/0 update-source FastEthernet 0/0
 address-family ipv6
  neighbor 3ffe::3 activate
  neighbor fe80::2%Ethernet1/0 activate
  exit-address-family
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a BGP neighboring router.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

neighbor version

To configure the Cisco IOS software to accept only a particular BGP version, use the **neighbor version** command in router configuration mode. To use the default version level of a neighbor, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **version** *number*

no neighbor {*ip-address* | *peer-group-name*} **version** *number*

Syntax Description

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
number	BGP version number. The version can be set to 2 to force the software to use only Version 2 with the specified neighbor. The default is to use Version 4 and dynamically negotiate down to Version 2 if requested.

Defaults

BGP Version 4

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Entering this command disables dynamic version negotiation.

Note The Cisco implementation of BGP in Cisco IOS Release 12.0(5)T or earlier releases supports BGP Versions 2, 3, and 4, with dynamic negotiation down to Version 2 if a neighbor does not accept BGP Version 4 (the default version).

The Cisco implementation of BGP in Cisco IOS Release 12.0(6)T or later releases supports BGP Version 4 only and does not support dynamic negotiation down to Version 2.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

The following example locks down to Version 4 of the BGP protocol:

```
router bgp 109
 neighbor 172.16.27.2 version 4
```

Related Commands

Command	Description
neighbor remote-as	Creates a BGP peer group.

neighbor weight

To assign a weight to a neighbor connection, use the **neighbor weight** command in address family or router configuration mode. To remove a weight assignment, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **weight** *number*

no neighbor {*ip-address* | *peer-group-name*} **weight** *number*

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
number	Weight to assign. Acceptable values are from 0 to 65535.

Defaults

Routes learned through another BGP peer have a default weight of 0 and routes sourced by the local router have a default weight of 32768.

Command Modes

Address family
Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
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

All routes learned from this neighbor will have the assigned weight initially. The route with the highest weight will be chosen as the preferred route when multiple routes are available to a particular network.

The weights assigned with the **set weight** route-map command override the weights assigned using the **neighbor weight** command.

Note For weight changes to take effect, use of the **clear ip bgp peer-group *** command may be necessary.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

The following router configuration mode example sets the weight of all routes learned via 172.16.12.1 to 50:

```
router bgp 109
 neighbor 172.16.12.1 weight 50
```

The following address family configuration mode example sets the weight of all routes learned via 172.16.12.1 to 50:

```
router bgp 109
address-family ipv4 multicast
 neighbor 172.16.12.1 weight 50
```

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 vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard Virtual Private Network (VPN) Version 4 address prefixes.
neighbor distribute-list	Distributes BGP neighbor information as specified in an access list.
neighbor filter-list	Sets up a BGP filter.
neighbor remote-as	Creates a BGP peer group.

network (BGP and multiprotocol BGP)

To specify the networks to be advertised by the Border Gateway Protocol (BGP) and multiprotocol BGP routing processes, use the **network** command in address family or router configuration mode. To remove an entry from the routing table, use the **no** form of this command.

network {*network-number* [**mask** *network-mask*] | *nsap-prefix*} [**route-map** *map-tag*]

no network {*network-number* [**mask** *network-mask*] | *nsap-prefix*} [**route-map** *map-tag*]

Syntax Description

network-number	Network that BGP or multiprotocol BGP will advertise.
mask *network-mask*	(Optional) Network or subnetwork mask with mask address.
nsap-prefix	Network service access point (NSAP) prefix of the Connectionless Network Service (CLNS) network that BGP or multiprotocol BGP will advertise. This argument is used only under NSAP address family configuration mode.
route-map *map-tag*	(Optional) Identifier of a configured route map. The route map should be examined to filter the networks to be advertised. If not specified, all networks are advertised. If the keyword is specified, but no route map tags are listed, no networks will be advertised.

Command Default

No networks are specified.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0	The limit of 200 network commands per BGP router was removed.
11.1(20)CC	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(7)T	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were removed. Address family configuration mode was added.
12.2(8)T	The *nsap-prefix* argument was added to address family configuration mode.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

BGP and multiprotocol BGP networks can be learned from connected routes, from dynamic routing, and from static route sources.

The maximum number of **network** commands you can use is determined by the resources of the router, such as the configured NVRAM or RAM.

Examples

The following example sets up network 10.108.0.0 to be included in the BGP updates:

```
router bgp 65100
 network 10.108.0.0
```

The following example sets up network 10.108.0.0 to be included in the multiprotocol BGP updates:

```
router bgp 64800
address family ipv4 multicast
 network 10.108.0.0
```

The following example advertises NSAP prefix 49.6001 in the multiprotocol BGP updates:

```
router bgp 64500
 address-family nsap
  network 49.6001
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enters the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family vpnv4	Enters the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
default-information originate (BGP)	Allows the redistribution of network 0.0.0.0 into BGP.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
router bgp	Configures the BGP routing process.

network backdoor

To specify a backdoor route to a BGP-learned prefix that provides better information about the network, use the **network backdoor** command in address family or router configuration mode. To remove an address from the list, use the **no** form of this command.

network *ip-address* **backdoor**

no network *ip-address* **backdoor**

Syntax Description

ip-address	IP address of the network to which you want a backdoor route.

Defaults

No network is marked as having a back door.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A backdoor network is assigned an administrative distance of 200. The objective is to make Interior Gateway Protocol (IGP) learned routes preferred. A backdoor network is treated as a local network, except that it is not advertised. A network that is marked as a back door is not sourced by the local router, but should be learned from external neighbors. The BGP best path selection algorithm does not change when a network is configured as a back door.

Examples

The following address family configuration example configures network 10.108.0.0 as a local network and network 192.168.7.0 as a backdoor network:

```
router bgp 109
address-family ipv4 multicast
 network 10.108.0.0
 network 192.168.7.0 backdoor
```

The following router configuration example configures network 10.108.0.0 as a local network and network 192.168.7.0 as a backdoor network:

```
router bgp 109
 network 10.108.0.0
 network 192.168.7.0 backdoor
```

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 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.
distance bgp	Allows the use of external, internal, and local administrative distances that could be a better route to a node.
network (BGP and multiprotocol BGP)	Specifies networks to be advertised by the BGP and multiprotocol BGP routing processes.
router bgp	Assigns an absolute weight to a BGP network.

redistribute (BGP to ISO IS-IS)

To redistribute routes from a Border Gateway Protocol (BGP) autonomous system into an International Organization for Standardization (ISO) Intermediate System-to-Intermediate System (IS-IS) routing process, use the **redistribute** command in router configuration mode. To remove the **redistribute** command from the configuration file and restore the system to its default condition where the software does not redistribute routes, use the **no** form of this command.

redistribute *protocol autonomous-system-number* [*route-type*] [**route-map** *map-tag*]

no redistribute *protocol autonomous-system-number* [*route-type*] [**route-map** *map-tag*]

Syntax Description

protocol	Source protocol from which routes are being redistributed. It must be the **bgp** keyword. The **bgp** keyword is used to redistribute dynamic routes.
autonomous-system-number	The autonomous system number of the BGP routing process. The range of values for this argument is any valid autonomous system number from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command.
route-type	(Optional) The type of route to be redistributed. It can be one of the following keywords: **clns** or **ip**. The default is **ip.** The **clns** keyword is used to redistribute BGP routes with network service access point (NSAP) addresses into IS-IS. The **ip** keyword is used to redistribute BGP routes with IP addresses into IS-IS.
route-map *map-tag*	(Optional) Identifier of a configured route map. The route map should be examined to filter the importation of routes from this source routing protocol to IS-IS. If not specified, all routes are redistributed. If the keyword is specified, but no route map tags are listed, no routes will be imported.

Command Default

Route redistribution is disabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(8)T	This command was modified. The **clns** keyword was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added. Support for changing autonomous system number of the BGP routing process was removed.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

The **clns** keyword must be specified to redistribute NSAP prefix routes from BGP into an ISO IS-IS routing process. This version of the **redistribute** command is used only under router configuration mode for IS-IS processes.

In redistribution from IGP (for example, ISIS, OSPF, RIP, or EIGRP) to BGP, the support for changing the autonomous system numbers of BGP from one to another is removed.

Examples

The following example configures NSAP prefix routes from BGP autonomous system 64500 to be redistributed into the IS-IS routing process called osi-proc-17:

```
router isis osi-proc-17
 redistribute bgp 64500 clns
```

In the following example the autonomous system BGP is modified from 200 to 300, this is not supported.

```
Router#config terminal
Router(config-if)#router eigrp 101
Router(config-router)#redistribute bgp 200
Router(config-router)#redistribute bgp 300
Cannot configure or redistribute to BGP AS 300
Please do "no router bgp 200" first
```

Remove support for autonomous system number 200 before configuring number 300.

```
Router(config)#no router bgp 200
Router(config-router)#redistribute bgp 300
```

Related Commands

Command	Description
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
router bgp	Configures the BGP routing process.
show route-map	Displays all route maps configured or only the one specified.

redistribute (IP)

To redistribute routes from one routing domain into another routing domain, use the **redistribute** command in the appropriate configuration mode. To disable redistribution, use the **no** form of this command.

redistribute *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*autonomous-system-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] [**nssa-only**]

no redistribute *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*autonomous-system-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] [**nssa-only**]

Syntax Description

protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, **connected**, **eigrp**, **isis**, **mobile**, **ospf**, **static** [**ip**], or **rip**. The **static** [**ip**] keyword is used to redistribute IP static routes. The optional **ip** keyword is used when redistributing into the Intermediate System-to-Intermediate System (IS-IS) protocol. The **connected** keyword refers to routes that are established automatically by virtue of having enabled IP on an interface. For routing protocols such as Open Shortest Path First (OSPF) and IS-IS, these routes will be redistributed as external to the autonomous system.
process-id	(Optional) For the **bgp** or **eigrp** keyword, this is an autonomous system number, which is a 16-bit decimal number. For the **isis** keyword, this is an optional *tag* value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing. For the **ospf** keyword, this is an appropriate OSPF process ID from which routes are to be redistributed. This identifies the routing process. This value takes the form of a nonzero decimal number. For the **rip** keyword, no *process-id* value is needed. By default, no process ID is defined.
level-1	Specifies that, for IS-IS, Level 1 routes are redistributed into other IP routing protocols independently.
level-1-2	Specifies that, for IS-IS, both Level 1 and Level 2 routes are redistributed into other IP routing protocols.
level-2	Specifies that, for IS-IS, Level 2 routes are redistributed into other IP routing protocols independently.

autonomous-system-number	(Optional) Autonomous system number for the redistributed route. 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.
metric *metric-value*	(Optional) When redistributing from one OSPF process to another OSPF process on the same router, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified. The default value is 0.
metric transparent	(Optional) Causes RIP to use the routing table metric for redistributed routes as the RIP metric.
metric-type *type-value*	(Optional) For OSPF, specifies the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values: • **1**—Type 1 external route • **2**—Type 2 external route If a **metric-type** is not specified, the Cisco IOS software adopts a Type 2 external route. For IS-IS, it can be one of two values: • **internal**—IS-IS metric that is < 63. • **external**—IS-IS metric that is > 64 < 128. The default is **internal**.
match {**internal** | **external 1** | **external 2**}	(Optional) For the criteria by which OSPF routes are redistributed into other routing domains. It can be one of the following: • **internal**—Routes that are internal to a specific autonomous system. • **external 1**—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external route. • **external 2**—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external route. The default is internal and external 1.

tag *tag-value*	(Optional) Specifies the 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between Autonomous System Boundary Routers (ASBRs). If none is specified, then the remote autonomous system number is used for routes from Border Gateway Protocol (BGP) and Exterior Gateway Protocol (EGP); for other protocols, zero (0) is used.
route-map	(Optional) Specifies the route map that should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. If not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.
map-tag	(Optional) Identifier of a configured route map.
subnets	(Optional) For redistributing routes into OSPF, the scope of redistribution for the specified protocol. By default, no subnets are defined.
nssa-only	(Optional) Sets the nssa-only attribute for all routes redistributed into OSPF.

Command Default

Route redistribution is disabled.

Command Modes

Router configuration (config-router)
Address family configuration (config-af)
Address family topology configuration (config-router-af-topology)

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	This command was modified. Address family configuration mode was added.
12.0(22)S	This command was modified. Address family support under EIGRP was added.
12.2(15)T	This command was modified. Address family support under EIGRP was added.
12.2(18)S	This command was modified. Address family support under EIGRP was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. This command was made available in router address family topology configuration mode.
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.

Release	Modification
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is 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 asplain.
Cisco IOS Release 15.0(1)M	This command was modified. The **nssa-only** keyword was added.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

A router receiving a link-state protocol with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

Routes learned from IP routing protocols can be redistributed at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

Redistributed routing information must be filtered by the **distribute-list out** router configuration command. This guideline ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

Whenever you use the **redistribute** or the **default-information** router configuration commands to redistribute routes into an OSPF routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a *default route* into the OSPF routing domain.

When routes are redistributed into OSPF from protocols other than OSPF or BGP, and no metric has been specified with the **metric-type** keyword and *type-value* argument, OSPF will use 20 as the default metric. When routes are redistributed into OSPF from BGP, OSPF will use 1 as the default metric. When routes are redistributed from one OSPF process to another OSPF process, Autonomous system (AS) external and not-so-stubby-area (NSSA) routes will use 20 as the default metric. When intra-area and inter-area routes are redistributed between OSPF processes, the internal OSPF metric from the redistribution source process is advertised as the external metric in the redistribution destination process. (This is the only case in which the routing table metric will be preserved when routes are redistributed into OSPF.)

When routes are redistributed into OSPF, only routes that are not subnetted are redistributed if the **subnets** keyword is not specified.

On a router internal to an NSSA area, the **nssa-only** keyword causes the originated type-7 NSSA LSAs to have their propagate (P) bit set to zero, which prevents area border routers from translating these LSAs into type-5 external LSAs. On an area border router that is connected to a NSSA and normal areas, the **nssa-only** keyword causes the routes to be redistributed only into the NSSA areas.

Routes configured with the **connected** keyword affected by this **redistribute** command are the routes not specified by the **network** router configuration command.

You cannot use the **default-metric** command to affect the metric used to advertise connected routes.

Note The **metric** value specified in the **redistribute** command supersedes the **metric** value specified using the **default-metric** command.

Default redistribution of IGPs or EGP into BGP is not allowed unless the **default-information originate** router configuration command is specified.

Using the no Form of the redistribute Command

Removing options that you have configured for the **redistribute** command requires careful use of the **no** form of the **redistribute** command to ensure that you obtain the result that you are expecting. See the "Examples" section for more information.

Release 12.2(33)SRB

If you plan to configure the Multi-Topology Routing (MTR) feature, you need to enter the **redistribute** command in router address family topology configuration mode in order for this OSPF router configuration command to become topology-aware.

4-Byte Autonomous System Number Support

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2, for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

The following example shows how OSPF routes are redistributed into a BGP domain:

```
Router(config)# router bgp 109
Router(config-router)# redistribute ospf
```

The following example causes EIGRP routes to be redistributed into an OSPF domain:

```
Router(config)# router ospf 110
Router(config-router)# redistribute eigrp
```

The following example causes the specified EIGRP process routes to be redistributed into an OSPF domain. The EIGRP-derived metric will be remapped to 100 and RIP routes to 200.

```
Router(config)# router ospf 109
Router(config-router)# redistribute eigrp 108 metric 100 subnets
Router(config-router)# redistribute rip metric 200 subnets
```

The following example configures BGP routes to be redistributed into IS-IS. The link-state cost is specified as 5, and the metric type will be set to external, indicating that it has lower priority than internal metrics.

```
Router(config)# router isis
Router(config-router)# redistribute bgp 120 metric 5 metric-type external
```

In the following example, network 172.16.0.0 will appear as an external link-state advertisement (LSA) in OSPF 1 with a cost of 100 (the cost is preserved):

```
Router(config)# interface ethernet 0
Router(config-if)# ip address 172.16.0.1 255.0.0.0
Router(config)# ip ospf cost 100
Router(config)# interface ethernet 1
Router(config-if)# ip address 10.0.0.1 255.0.0.0
!
Router(config)# router ospf 1
Router(config-router)# network 10.0.0.0 0.255.255.255 area 0
Router(config-router)# redistribute ospf 2 subnet
Router(config)# router ospf 2
Router(config-router)# network 172.16.0.0 0.255.255.255 area 0
```

The following example shows how BGP routes are redistributed into OSPF and assigned the local 4-byte autonomous system number in asplain format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Router(config)# router ospf 2
Router(config-router)# redistribute bgp 65538
```

The following example removes the **connected metric 1000 subnets** options from the **redistribute connected metric 1000 subnets** command and leaves the **redistribute connected** command in the configuration:

```
Router(config-router)# no redistribute connected metric 1000 subnets
```

The following example removes the **metric 1000** options from the **redistribute connected metric 1000 subnets** command and leaves the **redistribute connected subnets** command in the configuration:

```
Router(config-router)# no redistribute connected metric 1000
```

The following example removes the **subnets** options from the **redistribute connected metric 1000 subnets** command and leaves the **redistribute connected metric 1000** command in the configuration:

```
Router(config-router)# no redistribute connected subnets
```

The following example removes the **redistribute connected** command, and any of the options that were configured for the **redistribute connected** command, from the configuration:

```
Router(config-router)# no redistribute connected
```

The following example shows how EIGRP routes are redistributed into an EIGRP process in a named EIGRP configuration:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 1
Router(config-router-af)# topology base
Router(config-router-af-topology)# redistribute eigrp 6473 metric 1 1 1 1 1
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
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.

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 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.
default-information originate (BGP)	Allows the redistribution of network 0.0.0.0 into BGP.
default-information originate (IS-IS)	Generates a default route into an IS-IS routing domain.
default-information originate (OSPF)	Generates a default route into an OSPF routing domain.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
router bgp	Configures the BGP routing process.
router eigrp	Configures the EIGRP address-family process.
show route-map	Displays all route maps configured or only the one specified.
topology (EIGRP)	Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.

redistribute (ISO IS-IS to BGP)

To redistribute routes from an International Organization for Standardization (ISO) Intermediate System-to-Intermediate System (IS-IS) routing process into a Border Gateway Protocol (BGP) autonomous system, use the **redistribute** command in address family or router configuration mode. To remove the **redistribute** command from the configuration file and restore the system to its default condition where the software does not redistribute routes, use the **no** form of this command.

redistribute *protocol* [*process-id*] [*route-type*] [**route-map** [*map-tag*]]

no redistribute *protocol* [*process-id*] [*route-type*] [**route-map** [*map-tag*]]

Syntax Description

protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **isis** or **static**. The **isis** keyword is used to redistribute dynamic routes. The **static** keyword is used to redistribute static routes.
process-id	(Optional) When IS-IS is used as a source protocol, this argument defines a meaningful name for a routing process. The *process-id* argument identifies from which IS-IS routing process routes will be redistributed. Routes can be redistributed only from IS-IS routing processes that involve Level 2 routes, including IS-IS Level 1-2 and Level 2 routing processes. The *process-id* argument is not used when the protocol keyword is **static**.
route-type	(Optional) The type of route to be redistributed. It can be one of the following keywords: **clns** or **ip**. The default is **ip**. The **clns** keyword is used to redistribute Connectionless Network Service (CLNS) routes with network service access point (NSAP) addresses into BGP. The **ip** keyword is used to redistribute IS-IS routes with IP addresses into BGP.
route-map *map-tag*	(Optional) Identifier of a configured route map. The route map should be examined to filter the importation of routes from this source routing protocol to BGP. If no route map is specified, all routes are redistributed. If the **route-map** keyword is specified, but no *map-tag* value is entered, no routes will be imported.

Command Default

Route redistribution is disabled.

route-type: **ip**
route-map *map-tag*: If the **route-map** argument is not entered, all routes are redistributed; if no *map-tag* value is entered, no routes are imported.

Command Modes

Address family configuration (Cisco IOS 12.3(8)T and later releases)
Router configuration (T-releases after Cisco IOS 12.3(8)T)

Command History

Release	Modification
12.2(8)T	The **clns** keyword was added.
12.3(8)T	Beginning with Cisco IOS Release 12.3(8)T this version of the **redistribute** command should be entered under address family mode rather than router configuration mode.
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 **clns** keyword must be specified to redistribute NSAP prefix routes from an ISO IS-IS routing process into BGP. Beginning with Cisco IOS Release 12.3(8)T, this version of the **redistribute** command is entered only in address family configuration mode for BGP processes.

Examples

Cisco IOS Releases Prior to Release 12.3(8)T

The following example configures CLNS NSAP routes from the IS-IS routing process called osi-proc-6 to be redistributed into BGP:

```
Router(config)# router bgp 64352
Router(config-router)# redistribute isis osi-proc-6 clns
```

Cisco IOS Releases 12.3(8)T and Later Releases

The following example configures CLNS NSAP routes from the IS-IS routing process called osi-proc-15 to be redistributed into BGP:

```
Router(config)# router bgp 404
Router(config-router)# address-family nsap
Router(config-router-af)# redistribute isis osi-proc-15 clns
```

Related Commands

Command	Description
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
show route-map	Displays all route maps configured or only the one specified.

redistribute dvmrp

To configure redistribution of Distance Vector Multicast Routing Protocol (DVMRP) routes into multiprotocol BGP, use the **redistribute dvmrp** command in address family or router configuration mode. To stop such redistribution, use the **no** form of this command.

redistribute dvmrp [**route-map** *map-name*]

no redistribute dvmrp [**route-map** *map-name*]

Syntax Description

route-map *map-name*	(Optional) Name of the route map that contains various BGP attribute settings.

Defaults

DVMRP routes are not redistributed into multiprotocol BGP.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
11.1(20)CC	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command if you have a subset of DVMRP routes in an autonomous system that you want to take the multiprotocol BGP path. Define a route map to further specify which DVMRP routes get redistributed.

Examples

The following router configuration mode example redistributes DVMRP routes to BGP peers that match access list 1:

```
router bgp 109
 redistribute dvmrp route-map dvmrp-into-mbgp
route-map dvmrp-into-mbgp
 match ip address 1
```

The following address family configuration mode example redistributes DVMRP routes to multiprotocol BGP peers that match access list 1:

```
router bgp 109
address-family ipv4 multicast
 redistribute dvmrp route-map dvmrp-into-mbgp

route-map dvmrp-into-mbgp
 match ip address 1
```

router bgp

To configure the Border Gateway Protocol (BGP) routing process, use the **router bgp** command in global configuration mode. To remove a BGP routing process, use the **no** form of this command.

router bgp *autonomous-system-number*

no router bgp *autonomous-system-number*

Syntax Description

autonomous-system-number	Number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. 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 "Usage Guidelines" section.

Command Default

No BGP routing process is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was modified. Support for IPv6 was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(33)SB	This command was modified. Support for IPv6 was added.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.

Release	Modification
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

This command allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

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.

Note In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

Asdot Only Autonomous System Number Formatting

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, Cisco IOS XE Release 2.3, and later releases, the 4-octet (4-byte) autonomous system numbers are entered and displayed only in asdot notation, for example, 1.10 or 45000.64000. When using regular expressions to match 4-byte autonomous system numbers the asdot format includes a period which is a special character in regular expressions. A backslash must be entered before the period for example, 1\.14, to ensure the regular expression match does not fail. Table 6 shows

the format in which 2-byte and 4-byte autonomous system numbers are configured, matched in regular expressions, and displayed in **show** command output in Cisco IOS images where only asdot formatting is available.

Table 6 Asdot Only 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
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

Asplain as Default Autonomous System Number Formatting

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. Table 7 and Table 8 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 7 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 8 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

Reserved and Private Autonomous System Numbers

In Cisco IOS Release 12.0(32)S12, 12.0(32)SY8, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3 and later releases, the Cisco implementation of BGP supports RFC 4893. RFC 4893 was developed to allow BGP to support a gradual transition from 2-byte autonomous system numbers to 4-byte autonomous system numbers. A new reserved (private) autonomous system number, 23456, was created by RFC 4893 and this number cannot be configured as an autonomous system number in the Cisco IOS CLI.

RFC 5398, *Autonomous System (AS) Number Reservation for Documentation Use*, describes new reserved autonomous system numbers for documentation purposes. Use of the reserved numbers allow configuration examples to be accurately documented and avoids conflict with production networks if these configurations are literally copied. The reserved numbers are documented in the IANA autonomous system number registry. Reserved 2-byte autonomous system numbers are in the contiguous block, 64496 to 64511 and reserved 4-byte autonomous system numbers are from 65536 to 65551 inclusive.

Private 2-byte autonomous system numbers are still valid in the range from 64512 to 65534 with 65535 being reserved for special use. Private autonomous system numbers can be used for internal routing domains but must be translated for traffic that is routed out to the Internet. BGP should not be configured to advertise private autonomous system numbers to external networks. Cisco IOS software does not remove private autonomous system numbers from routing updates by default. We recommend that ISPs filter private autonomous system numbers.

Note Autonomous system number assignment for public and private networks is governed by the IANA. For information about autonomous-system numbers, including reserved number assignment, or to apply to register an autonomous system number, see the following URL: http://www.iana.org/.

Examples

The following example configures a BGP process for autonomous system 45000 and configures two external BGP neighbors in different autonomous systems using 2-byte autonomous system numbers:

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

The following example configures a BGP process for autonomous system 65538 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asplain notation. This example is supported 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.

```
router bgp 65538
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.3.2 remote-as 65550
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

The following example configures a BGP process for autonomous system 1.2 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asdot notation. This example is supported in Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, and Cisco IOS XE Release 2.3, and later releases.

```
router bgp 1.2
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.3.2 remote-as 1.14
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.

scope

To define the scope for a Border Gateway Protocol (BGP) routing session and to enter router scope configuration mode, use the **scope** command in router configuration mode. To remove the scope configuration, use the **no** form of this command.

scope {**global** | **vrf** *vrf-name*}

no scope {**global** | **vrf** *vrf-name*}

Syntax Description

global	Configures BGP to use the global routing table or a specific topology table.
vrf	Configures BGP to use a specific VRF routing table.
vrf-name	Name of an existing VRF.

Command Default

No scope is defined for a BGP routing session.

Command Modes

Router configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

A new configuration hierarchy, named scope, has been introduced into the BGP protocol. To implement Multi-Topology Routing (MTR) support for BGP, the scope hierarchy is required, but the scope hierarchy is not limited to MTR use. The scope hierarchy introduces some new configuration modes such as router scope configuration mode. Router scope configuration mode is entered by configuring the **scope** command in router configuration mode, and a collection of routing tables is created when this command is entered. The scope is configured to isolate routing calculation for a single network (globally) or on a per-VRF basis, and BGP commands configured in routing scope configuration mode are referred to as scoped commands. The scope hierarchy can contain one or more address families.

The BGP command-line interface (CLI) has been modified to provide backwards compatibility for pre-MTR BGP configuration and to provide a hierarchal implementation of MTR. From router scope configuration mode, MTR is configured first by entering the **address-family** command to enter the desired address family and then by entering the **topology** command to define the topology

Note Configuring a scope for a BGP routing process removes CLI support for pre-MTR-based configuration.

Examples

The following example defines a global scope that includes both unicast and multicast topology configurations. Another scope is specifically defined only for the VRF named DATA.

```
Router(config)# router bgp 45000
Router(config-router)# scope global
Router(config-router-scope)# bgp default ipv4-unicast
```

```
Router(config-router-scope)# neighbor 172.16.1.2 remote-as 45000
Router(config-router-scope)# neighbor 192.168.3.2 remote-as 50000
Router(config-router-scope)# address-family ipv4 unicast
Router(config-router-scope-af)# topology VOICE
Router(config-router-scope-af)# bgp tid 100
Router(config-router-scope-af)# neighbor 172.16.1.2 activate
Router(config-router-scope-af)# exit
Router(config-router-scope)# address-family ipv4 multicast
Router(config-router-scope-af)# topology base
Router(config-router-scope-af-topo)# neighbor 192.168.3.2 activate
Router(config-router-scope-af-topo)# exit
Router(config-router-scope-af)# exit
Router(config-router-scope)# exit
Router(config-router)# scope vrf DATA
Router(config-router-scope)# neighbor 192.168.1.2 remote-as 40000
Router(config-router-scope)# address-family ipv4
Router(config-router-scope-af)# neighbor 192.168.1.2 activate
Router(config-router-scope-af)# end
```

Related Commands

Command	Description
bgp tid	Configures BGP to accept routes with a specified topology ID.
topology (BGP)	Configures a process to route IP traffic under the specified topology instance.

set as-path

To modify an autonomous system path for BGP routes, use the **set as-path** command in route-map configuration mode. To not modify the autonomous system path, use the **no** form of this command.

set as-path {**tag** | **prepend** *as-path-string*}

no set as-path {**tag** | **prepend** *as-path-string*}

Syntax Description

tag	Converts the tag of a route into an autonomous system path. Applies only when redistributing routes into BGP.
prepend	Appends the string following the keyword **prepend** to the autonomous system path of the route that is matched by the route map. Applies to inbound and outbound BGP route maps.
as-path-string	Number of an autonomous system to prepend to the AS_PATH attribute. The range of values for this argument is any valid autonomous system number from 1 to 65535. Multiple values can be entered; up to 10 AS numbers can be entered. • 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

An autonomous system path is not modified.

Command Modes

Route-map configuration (config-route-map)

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.
12.2(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.

Release	Modification
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

The only global BGP metric available to influence the best path selection is the autonomous system path length. By varying the length of the autonomous system path, a BGP speaker can influence the best path selection by a peer further away.

By allowing you to convert the tag into an autonomous system path, the **set as-path tag** variation of this command modifies the autonomous system length. The **set as-path prepend** variation allows you to "prepend" an arbitrary autonomous system path string to BGP routes. Usually the local autonomous system number is prepended multiple times, increasing the autonomous system path length.

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.

Examples

The following example converts the tag of a redistributed route into an autonomous system path:

```
route-map set-as-path-from-tag
 set as-path tag
!
router bgp 100
 redistribute ospf 109 route-map set-as-path-from-tag
```

The following example prepends 100 100 100 to all the routes that are advertised to 10.108.1.1:

```
route-map set-as-path
 match as-path 1
 set as-path prepend 100 100 100
!
router bgp 100
 neighbor 10.108.1.1 route-map set-as-path out
```

The following example prepends 65538, 65538, and 65538 to all the routes that are advertised to 192.168.1.2. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
route-map set-as-path
 match as-path 1.1
 set as-path prepend 65538 65538 65538
 exit
router bgp 65538
 neighbor 192.168.1.2 route-map set-as-path out
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
router bgp	Configures the BGP routing process.
set tag (IP)	Sets a tag value of the destination routing protocol.

set comm-list delete

To remove communities from the community attribute of an inbound or outbound update, use the **set comm-list delete** command in route-map configuration mode. To remove a previous **set comm-list delete** command, use the **no** form of this command.

set comm-list {*community-list-number* | *community-list-name*} **delete**

no set comm-list {*community-list-number* | *community-list-name*} **delete**

Syntax Description

community-list-number	A standard or expanded community list number. The range of standard community list numbers is from 1 to 99. The range of expanded community list number is from 100 to 500.
community-list-name	A standard or expanded community list name.

Command Default

No communities are removed.

Command Modes

Route-map configuration

Command History

Release	Modification
12.0	This command was introduced.
12.0(10)S	Named community list support was added.
12.0(16)ST	Named community list support was integrated into Cisco IOS Release 12.0(16)ST.
12.1(9)E	Named community list support was integrated into Cisco IOS Release 12.1(9)E.
12.2(8)T	Named community list support was integrated into Cisco IOS Release 12.2(8)T.
12.0(22)S	The maximum number of expanded community lists was increased from 199 to 500 in Cisco IOS Release 12.0(22)S.
12.2(14)S	The maximum number of expanded community lists was increased from 199 to 500 and named community list support were integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	The maximum number of expanded community lists was increased from 199 to 500 in Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This **set** route-map configuration command removes communities from the community attribute of an inbound or outbound update using a route map to filter and determine the communities to be deleted. Depending upon whether the route map is applied to the inbound or outbound update for a neighbor, each community that passes the route map **permit** clause and matches the given community list will be removed from the community attribute being received from or sent to the Border Gateway Protocol (BGP) neighbor.

Each entry of a standard community list should list only one community when used with the **set comm-list delete** command. For example, in order to be able to delete communities 10:10 and 10:20, you must use the following format to create the entries:

```
ip community-list 500 permit 10:10
ip community-list 500 permit 10:20
```

The following format for a community list entry, while acceptable otherwise, does not work with the **set comm-list delete** command:

```
config ip community-list 500 permit 10:10 10:20
```

When both the **set community** *community-number* and **set comm-list delete** commands are configured in the same sequence of a route map attribute, the deletion operation (**set comm-list delete**) is performed before the set operation (**set community** *community-number*).

Examples

In the following example, the communities 100:10 and 100:20 (if present) will be deleted from updates received from 172.16.233.33. Also, except for 100:50, all communities beginning with 100: will be deleted from updates sent to 172.16.233.33.

```
router bgp 100
 neighbor 172.16.233.33 remote-as 120
 neighbor 172.16.233.33 route-map ROUTEMAPIN in
 neighbor 172.16.233.33 route-map ROUTEMAPOUT out
!
ip community-list 500 permit 100:10
ip community-list 500 permit 100:20
!
ip community-list 120 deny   100:50
ip community-list 120 permit 100:.*
!
route-map ROUTEMAPIN permit 10
 set comm-list 500 delete
!
route-map ROUTEMAPOUT permit 10
 set comm-list 120 delete
```

Related Commands

Command	Description
set community	Sets the BGP communities attribute.

set community

To set the BGP communities attribute, use the **set community** route map configuration command. To delete the entry, use the **no** form of this command.

set community {*community-number* [**additive**] [*well-known-community*] | **none**}

no set community

Syntax Description

community-number	Specifies that community number. Valid values are from 1 to 4294967200, **no-export**, or **no-advertise**.
additive	(Optional) Adds the community to the already existing communities.
well-known-community	(Optional) Well know communities can be specified by using the following keywords: • internet • local-as • no-advertise • no-export
none	(Optional) Removes the community attribute from the prefixes that pass the route map.

Command Default

No BGP communities attributes exist.

Command Modes

Route-map configuration

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.
12.2SX	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

You must have a match clause (even if it points to a “permit everything” list) if you want to set tags.

Use the **route-map** global configuration command, and the **match** and **set** route map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route map configuration commands specify the redistribution *set actions* to be performed when all of the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

In the following example, routes that pass the autonomous system path access list 1 have the community set to 109. Routes that pass the autonomous system path access list 2 have the community set to no-export (these routes will not be advertised to any external BGP [eBGP] peers).

```
route-map set_community 10 permit
 match as-path 1
 set community 109

route-map set_community 20 permit
 match as-path 2
 set community no-export
```

In the following similar example, routes that pass the autonomous system path access list 1 have the community set to 109. Routes that pass the autonomous system path access list 2 have the community set to local-as (the router will not advertise this route to peers outside the local autonomous system.

```
route-map set_community 10 permit
 match as-path 1
 set community 109

route-map set_community 20 permit
 match as-path 2
 set community local-as
```

Related Commands

Command	Description
ip community-list	Creates a community list for BGP and control access to it.
match community	Matches a BGP community.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set comm-list delete	Removes communities from the community attribute of an inbound or outbound update.
show ip bgp community	Displays routes that belong to specified BGP communities.

set dampening

To set the BGP route dampening factors, use the **set dampening** route map configuration command. To disable this function, use the **no** form of this command.

set dampening *half-life reuse suppress max-suppress-time*

no set dampening

Syntax Description

half-life	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 from 1 to 45 minutes. The default is 15 minutes.
reuse	Unsuppresses the route if the penalty for a flapping route decreases enough to fall below this value. 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	Suppresses a route when its penalty exceeds this limit. The range is from 1 to 20000; the default is 2000.
max-suppress-time	Maximum time (in minutes) a route can be suppressed. The range is from 1 to 20000; the default is four times the *half-life* value. If the *half-life* value is allowed to default, the maximum suppress time defaults to 60 minutes.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

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

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

When a BGP peer is reset, the route is withdrawn and the flap statistics cleared. In this instance, the withdrawal does not incur a penalty even though route flap dampening is enabled.

Examples

The following example sets the half life to 30 minutes, the reuse value to 1500, the suppress value to 10000; and the maximum suppress time to 120 minutes:

```
route-map tag
 match as path 10
 set dampening 30 1500 10000 120
!
router bgp 100
 neighbor 172.16.233.52 route-map tag in
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set ip next-hop	Specifies the address of the next hop.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set origin (BGP)	Sets the BGP origin code.
set tag (IP)	Sets the value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.
show route-map	Displays all route maps configured or only the one specified.

set extcommunity

To set Border Gateway Protocol (BGP) extended community attributes, use the **set extcommunity** command in route-map configuration mode. To delete the entry, use the **no** form of this command.

set extcommunity {**rt** [*extended-community-value*] [**additive**] | **soo** [*extended-community-value*]}

no set extcommunity

Syntax Description

rt	Specifies the route target (RT) extended community attribute.
soo	Specifies the site of origin (SOO) extended community attribute.
extended-community-value	(Optional) Specifies the value to be set. The value can be one of the following combinations: • *autonomous-system-number*:*network-number* • *ip-address*:*network-number* • *ipv6-address*:*network-number* The colon is used to separate the autonomous system number and network number, the IP address and network number, or the IPv6 address and network number. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 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.
additive	(Optional) Adds a route target to the existing route target list without replacing any existing route targets.

Command Default

Specifying new route targets with the **rt** keyword replaces existing route targets by default, unless the **additive** keyword is used. The use of the **additive** keyword adds the new route target to the existing route target list but does not replace any existing route targets.

Command Modes

Route-map configuration (config-route-map)

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.
12.2(33)SRB	Support for IPv6 was added.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	Support for IPv6 was added. and this command was integrated into Cisco IOS Release 12.2(33)SB.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).

The **set extcommunity** command is used to configure set clauses that use extended community attributes in route maps. All of the standard rules of match and set clauses apply to the configuration of extended community attributes.

The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.

The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the Provider Edge (PE) router learned the route. All routes learned from a particular site must be assigned the same SOO extended community attribute, whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO can be applied to routes that are learned from VRFs. The SOO should not be configured for stub sites or sites that are not multihomed.

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.

Examples

The following example sets the route target to extended community attribute 100:2 for routes that are permitted by the route map:

```
Router(config)# access-list 2 permit 192.168.78.0 255.255.255.0
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match ip-address 2
Router(config-route-map)# set extcommunity rt 100:2
```

The following example sets the route target to extended community attribute 100:3 for routes that are permitted by the route map. The use of the **additive** keyword adds route target 100:3 to the existing route target list but does not replace any existing route targets.

```
Router(config)# access-list 3 permit 192.168.79.0 255.255.255.0
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match ip-address 3
Router(config-route-map)# set extcommunity rt 100:3 additive
```

Note Configuring route targets with the **set extcommunity** command will replace existing route targets, unless the **additive** keyword is used.

The following example sets the site of origin to extended community attribute 100:4 for routes that are permitted by the route map:

```
Router(config)# access-list 4 permit 192.168.80.0 255.255.255.0
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match ip-address 4
Router(config-route-map)# set extcommunity soo 100:4
```

In IPv6, the following example sets the SoO to extended community attribute 100:28 for routes that are permitted by the route map:

```
(config)# router bgp 100
(config-router)# address-family ipv6 vrf red
(config-router-af)# neighbor 8008::72a route-map setsoo in
(config-router-af)# exit
(config-router)# route-map setsoo permit 10
(config-router)# set extcommnunity soo 100:28
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, shows how to create a VRF with a route-target that uses a 4-byte autonomous system number, 65537 in asplain format, and how to set the route-target to extended community value 65537:100 for routes that are permitted by the route map.

```
Router(config)# ip vrf vpn_red
Router(config-vrf)# rd 64500:100
Router(config-vrf)# route-target both 65537:100
Router(config-vrf)# exit
Router(config)# route-map rt_map permit 10
Router(config-route-map)# set extcommunity rt 65537:100
Router(config-route-map)# end
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3, and later releases, shows how to create a VRF with a route-target that uses a 4-byte autonomous system number, 1.1 in asdot format, and how to set the SoO to extended community attribute 1.1:100 for routes that are permitted by the route map.

```
Router(config)# ip vrf vpn_red
Router(config-vrf)# rd 64500:100
Router(config-vrf)# route-target both 1.1:100
Router(config-vrf)# exit
Router(config)# route-map soo_map permit 10
Router(config-route-map)# set extcommunity soo 1.1:100
Router(config-route-map)# 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.
ip extcommunity-list	Creates an extended community list and controls access to it.
match extcommunity	Matches a BGP VPN extended community list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
router bgp	Configures the BGP routing process.
route-target	Creates a route target extended community for a VRF.
show ip extcommunity-list	Displays routes that are permitted by the extended community list.
show route-map	Displays all route maps configured or only the one specified.

set extcommunity cost

To create a set clause to apply the cost community attribute to routes that pass through a route map, use the **set extcommunity cost** command in route-map configuration mode. To delete the cost community set clause, use the **no** form of this command.

set extcommunity cost [**igp** | **pre-bestpath**] *community-id cost-value*

no set extcommunity cost [**igp**] *community-id cost-value*

Syntax Description

igp	(Optional) Specifies the IGP point of insertion (POI). The configuration of this keyword forces the cost community to be evaluated after the IGP distance to the next hop has been compared. If this keyword is not specified, IGP is the default POI.
community-id	The ID for the configured extended community. The range is from 0 to 255.
cost-value	The configured cost that is set for matching paths in the route map. The range is from 0 to 4294967295.

Command Default

The default cost value is applied to routes that are not configured with the cost community attribute when cost community filtering is enabled. The default *cost-value* is half of the maximum value (4294967295) or 2147483647.

Command Modes

Route-map configuration

Command History

Release	Modification
12.0(24)S	This command was introduced into Cisco IOS Release 12.0(24)S.
12.3(2)T	This command was integrated.
12.2(18)S	This command was integrated.
12.0(27)S	Support for mixed EIGRP MPLS VPN network topologies that contain back door routes was introduced into Cisco IOS Release 12.0(27)S.
12.3(8)T	Support for mixed EIGRP MPLS VPN network topologies that contain back door routes was introduced into Cisco IOS Release 12.3(8)T.
12.2(25)S	Support for mixed EIGRP MPLS VPN network topologies that contain back door routes was introduced into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The cost community attribute is applied to internal routes by configuring the **set extcommunity cost** command in a route map. The cost community set clause is configured with a cost community ID number (0-255) and a cost community number value (0-4294967295). The path with the lowest cost community number is preferred. In the case where two paths have been configured with the same cost community value, the path selection process will then prefer the path with the lower community ID.

The BGP Cost Community feature can be configured only within the same autonomous-system or confederation. The cost community is a non-transitive extended community. The cost community is passed to internal BGP (iBGP) and confederation peers only and is not passed to external BGP (eBGP) peers. The cost community allows you to customize the local preference and best path selection process for specific paths. The cost extended community attribute is propagated to iBGP peers when extended community exchange is enabled with the **neighbor send-community** command.

The following commands can be used to apply the route map with the cost community set clause:

- **aggregate-address**
- **neighbor default-originate route-map** {**in** | **out**}
- **neighbor route-map**
- **network route-map**
- **redistribute route-map**

Multiple cost community set clauses may be configured with the **set extcommunity cost** command in a single route map block or sequence. However, each set clause must be configured with a different ID value for each point of insertion (POI).

Aggregate routes and multipaths are supported by the BGP Cost Community feature. The cost community attribute can be applied to either type of route. The cost community attribute is passed to the aggregate or multipath route from component routes that carry the cost community attribute. Only unique IDs are passed, and only the highest cost of any individual component route will be applied to the aggregate on a per-ID basis. If multiple component routes contain the same ID, the highest configured cost is applied to the route. If one or more component routes does not carry the cost community attribute or if the component routes are configured with different IDs, then the default value (2147483647) will be advertised for the aggregate or multipath route.



Note The BGP cost community attribute must be supported on all routers in an autonomous system or confederation before cost community filtering is configured. The cost community should be applied consistently throughout the local autonomous system or confederation to avoid potential routing loops.

Support for EIGRP MPLS VPN Back Door Links

The “pre-bestpath” point of insertion (POI) has been introduced in the BGP Cost Community feature to support mixed EIGRP VPN network topologies that contain VPN and backdoor links. This POI is applied automatically to EIGRP routes that are redistributed into BGP. The “pre-best path” POI carries the EIGRP route type and metric. This POI influences the best path calculation process by influencing BGP to consider this POI before any other comparison step. No configuration is required. This feature is enabled automatically for EIGRP VPN sites when a supporting is installed to a PE, CE, or back door router.

Examples

The following example configuration shows the configuration of the **set extcommunity cost** command. The following example applies the cost community ID of 1 and cost community value of 100 to routes that are permitted by the route map. This configuration will cause the best path selection process to prefer this route over other equal cost paths that were not permitted by this route map sequence.

```
Router(config)# router bgp 50000
Router(config-router)# neighbor 10.0.0.1 remote-as 50000
Router(config-router)# neighbor 10.0.0.1 update-source Loopback 0
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 10.0.0.1 activate
Router(config-router-af)# neighbor 10.0.0.1 route-map COST1 in
Router(config-router-af)# neighbor 10.0.0.1 send-community both
Router(config-router-af)# exit
Router(config)# route-map COST1 permit 10
Router(config-route-map)# match ip-address 1
Router(config-route-map)# set extcommunity cost 1 100
```

Related Commands

Command	Description
aggregate-address	Creates an aggregate entry in a BGP or multicast BGP database.
bgp bestpath cost-community ignore	Configures a router that is running BGP to not evaluate the cost community attribute during the best path selection process.
neighbor default-originate	Allows a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.
neighbor route-map	Applies a route map to incoming or outgoing routes.
network (BGP and multiprotocol BGP)	Specifies the networks to be advertised by the BGP and multiprotocol BGP routing processes.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
show ip bgp	Displays entries in the BGP routing table.

set ip next-hop (BGP)

To indicate where to output packets that pass a match clause of a route map for policy routing, use the **set ip next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ip next-hop *ip-address* [*... ip-address*] [**peer-address**]

no set ip next-hop *ip-address* [*... ip-address*] [**peer-address**]

Syntax Description

ip-address	IP address of the next hop to which packets are output. It need not be an adjacent router.
peer-address	(Optional) Sets the next hop to be the BGP peering address.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0	The **peer-address** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *ip-address* argument.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

If the first next hop specified with the **set ip next-hop** command is down, the optionally specified IP addresses are tried in turn.

When the **set ip next-hop command** is used with the **peer-address** keyword in an inbound route map of a BGP peer, the next hop of the received matching routes will be set to be the neighbor peering address, overriding any third-party next hops. So the same route map can be applied to multiple BGP peers to override third-party next hops.

When the **set ip next-hop** command is used with the **peer-address** keyword in an outbound route map of a BGP peer, the next hop of the advertised matching routes will be set to be the peering address of the local router, thus disabling the next hop calculation. The **set ip next-hop** command has finer granularity than the (per-neighbor) **neighbor next-hop-self** command, because you can set the next hop for some routes, but not others. The **neighbor next-hop-self** command sets the next hop for all routes sent to that neighbor.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**



Note To avoid a common configuration error for reflected routes, do not use the **set ip next-hop** command in a route map to be applied to BGP route reflector clients.

Examples

In the following example, three routers are on the same FDDI LAN (with IP addresses 10.1.1.1, 10.1.1.2, and 10.1.1.3). Each is in a different autonomous system. The **set ip next-hop peer-address** command specifies that traffic from the router (10.1.1.3) in remote autonomous system 300 for the router (10.1.1.1) in remote autonomous system 100 that matches the route map is passed through the router bgp 200, rather than sent directly to the router (10.1.1.1) in autonomous system 100 over their mutual connection to the LAN.

```
router bgp 200
neighbor 10.1.1.3 remote-as 300
neighbor 10.1.1.3 route-map set-peer-address out
neighbor 10.1.1.1 remote-as 100
route-map set-peer-address permit 10
set ip next-hop peer-address
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
neighbor next-hop-self	Disables next hop processing of BGP updates on the router.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol to another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and that have no explicit route to the destination.

set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.

set metric (BGP-OSPF-RIP)

To set the metric value for a routing protocol, use the **set metric** command in route-map configuration mode. To return to the default metric value, use the **no** form of this command.

set metric *metric-value*

no set metric *metric-value*

Syntax Description

metric-value	Metric value; an integer from –294967295 to 294967295. This argument applies to all routing protocols except Enhanced Interior Gateway Routing Protocol (EIGRP).

Defaults

The dynamically learned metric value.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

We recommend that you consult your Cisco technical support representative before changing the default value.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution *set actions* to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

The following example sets the metric value for the routing protocol to 100:

```
route-map set-metric
 set metric 100
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set ip next-hop	Specifies the address of the next hop.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set origin (BGP)	Sets the BGP origin code.
set tag (IP)	Sets the value of the destination routing protocol.

set metric-type internal

To set the Multi Exit Discriminator (MED) value on prefixes advertised to external BGP (eBGP) neighbors to match the Interior Gateway Protocol (IGP) metric of the next hop, use the **set metric-type internal** command in route-map configuration mode. To return to the default, use the **no** form of this command.

set metric-type internal

no set metric-type internal

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command will cause BGP to advertise a MED value that corresponds to the IGP metric associated with the next hop of the route. This command applies to generated, internal BGP (iBGP)-, and eBGP-derived routes.

If this command is used, multiple BGP speakers in a common autonomous system can advertise different MED values for a particular prefix. Also, note that if the IGP metric changes, BGP will readvertise the route every 10 minutes.

Use the **route-map** global configuration command and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution *set actions* to be performed when all of the match criteria of the route map are met. When all match criteria are met, all set actions are performed.

Note This command is not supported for redistributing routes into Border Gateway Protocol (BGP).

Examples

In the following example, the MED value for all the advertised routes to neighbor 172.16.2.3 is set to the corresponding IGP metric of the next hop:

```
router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 200
 neighbor 172.16.2.3 route-map setMED out
!
route-map setMED permit 10
 match as-path 1
 set metric-type internal
!
 ip as-path access-list 1 permit .*
```

Related Commands

Command	Description
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

set origin (BGP)

To set the BGP origin code, use the **set origin** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set origin {**igp** | **egp** *autonomous-system-number* | **incomplete**}

no set origin {**igp** | **egp** *autonomous-system-number* | **incomplete**}

Syntax Description

igp	Remote Interior Gateway Protocol (IGP) system.
egp	Local Exterior Gateway Protocol (EGP) system.
autonomous-system-number	Number of a remote autonomous system number. The range of values for this argument is any valid autonomous system number from 1 to 65535.
incomplete	Unknown heritage.

Command Default

The origin of the route is based on the path information of the route in the main IP routing table.

Command Modes

Route-map configuration (config-route-map)

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.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.4(2)T	This command was modified. The **egp** keyword and *autonomous-system-number* argument were removed.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

You must have a match clause (even if it points to a “permit everything” list) if you want to set the origin of a route. Use this command to set a specific origin when a route is redistributed into BGP. When routes are redistributed, the origin is usually recorded as incomplete, identified with a ? in the BGP table.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands

specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution *set actions* to be performed when all of the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

The following example sets the origin of routes that pass the route map to IGP:

```
route-map set_origin
 match as-path 10
 set origin igp
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
router bgp	Configures the BGP routing process.
set as-path	Modifies an autonomous system path for BGP routes.

set traffic-index

To indicate how to classify packets that pass a match clause of a route map for Border Gateway Protocol (BGP) policy accounting, use the **set traffic-index** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set traffic-index *bucket-number*

no set traffic-index *bucket-number*

Syntax Description

bucket-number	Number that represents a bucket into which packet and byte statistics are collected for a specific traffic classification. The range is from 1 to 64.

Command Default

Routing traffic is not classified.

Command Modes

Route-map configuration

Command History

Release	Modification
12.0(9)S	This command was introduced.
12.0(17)ST	This command was integrated into Cisco IOS Release 12.0(17)ST.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.0(22)S	Support for 64 buckets was added for the Cisco 12000 series Internet router.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T and support for 64 buckets was added for all platforms.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **set traffic-index** route-map configuration command, the **route-map** global configuration command, and a **match** route-map configuration command to define the conditions for BGP policy accounting. The **match** commands specify the *match criteria*—the conditions under which policy routing occurs. The **set traffic-index** command specifies the *set actions*—the particular routing actions to perform if the criteria specified by the **match** commands are met.

Examples

In the following example, an index for BGP policy accounting is set according to autonomous system path criteria:

```
route-map buckets permit 10
 match as-path 1
 set traffic-index 1
```

Related Commands

Command	Description
bgp-policy	Enables BGP policy accounting or policy propagation on an interface.
route-map	Defines the conditions for redistributing routes from one routing protocol to another, or enables policy routing.

set weight

To specify the BGP weight for the routing table, use the **set weight** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set weight *number*

no set weight *number*

Syntax Description

number	Weight value. It can be an integer ranging from 0 to 65535.

Defaults

The weight is not changed by the specified route map.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The implemented weight is based on the first matched autonomous system path. Weights indicated when an autonomous system path is matched override the weights assigned by global **neighbor** commands. In other words, the weights assigned with the **set weight** route-map configuration command override the weights assigned using the **neighbor weight** command.

Examples

The following example sets the BGP weight for the routes matching the autonomous system path access list to 200:

```
route-map set-weight
 match as-path 10
 set weight 200
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.

match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set ip next-hop	Specifies the address of the next hop.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set origin (BGP)	Sets the BGP origin code.
set tag (IP)	Sets the value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

show bgp all community

To display routes for all address families belonging to a particular Border Gateway Protocol (BGP) community, use the **show bgp all community** command in user EXEC or privileged EXEC configuration mode.

show bgp all community [*community-number...*[*community-number*]] [**local-as**] [**no-advertise**] [**no-export**] [**exact-match**]

Syntax Description

community-number	(Optional) Displays the routes pertaining to the community numbers specified. • You can specify multiple community numbers. The range is from 1 to 4294967295 or AA:NN (autonomous system:community number, which is a 2-byte number).
local-as	(Optional) Displays only routes that are not sent outside of the local autonomous system (well-known community).
no-advertise	(Optional) Displays only routes that are not advertised to any peer (well-known community).
no-export	(Optional) Displays only routes that are not exported outside of the local autonomous system (well-known community).
exact-match	(Optional) Displays only routes that match exactly with the BGP community list specified. **Note** The availability of keywords in the command depends on the command mode. The **exact-match** keyword is not available in user EXEC mode.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

You can enter the **local-as**, **no-advertise** and **no-export** keywords in any order. You can set the communities using the **set community** command.

When using the **bgp all community** command, be sure to enter the numerical communities before the well-known communities.

For example, the following string is not valid:

```
Router# show bgp all community local-as 111:12345
```

Use the following string instead:

```
Router# show bgp all community 111:12345 local-as
```

Examples

The following is sample output from the **show bgp all community** command, specifying communities of 1, 2345, and 6789012:

```
Router# show bgp all community 1 2345 6789012 no-advertise local-as no-export exact-match

For address family: IPv4 Unicast

BGP table version is 5, local router ID is 30.0.0.5
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
*> 10.0.3.0/24       10.0.0.4                               0 4 3 ?
*> 10.1.0.0/16       10.0.0.4                    0          0 4 ?
*> 10.12.34.0/24     10.0.0.6                    0          0 6 ?
```

Table 9 describes the significant fields shown in the display.

Table 9 show bgp all community Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	The router ID of the router on which the BGP communities are set to display. A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from the Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	The network address and network mask of a network entity. The type of address depends on the address family.

Table 9 show bgp all community Field Descriptions (continued)

Field	Description
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. The type of address depends on the address family.
Metric	The value of the inter autonomous system metric. This field is not used frequently.
LocPrf	Local preference value as set with the **set local-preference** command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Related Commands

Command	Description
set community	Sets BGP communities.
set local-preference	Specifies a preference value for the autonomous system path.

show bgp all neighbors

To display information about Border Gateway Protocol (BGP) connections to neighbors of all address families, use the **show bgp all neighbors** command in user EXEC or privileged EXEC mode.

show bgp all neighbors [*ip-address* | *ipv6-address*] [**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** [*reg-exp*] | **policy** [**detail**] | **received prefix-filter** | **received-routes** | **routes**]

Syntax Description

ip-address	(Optional) IP address of a neighbor. If this argument is omitted, information about all neighbors is displayed.
ipv6-address	(Optional) Address of the IPv6 BGP-speaking neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
advertised-routes	(Optional) Displays all routes that have been advertised to neighbors.
dampened-routes	(Optional) Displays the dampened routes received from the specified neighbor (for external BGP peers only).
flap-statistics	(Optional) Displays the flap statistics of the routes learned from the specified neighbor (for external BGP peers only).
paths *reg-exp*	(Optional) Displays autonomous system paths learned from the specified neighbor. An optional regular expression can be used to filter the output.
policy	(Optional) Displays the policies applied to neighbor per address family.
detail	(Optional) Displays detailed policy information such as route maps, prefix lists, community lists, Access Control Lists (ACLs), and autonomous system path filter lists.
received prefix-filter	(Optional) Displays the prefix-list (outbound route filter [ORF]) sent from the specified neighbor.
received-routes	(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	(Optional) Displays all routes that are received and accepted. The output displayed when this keyword is entered is a subset of the output displayed by the **received-routes** keyword.

Command Default

The output of this command displays information for all neighbors.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(26)	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S and was made available in privileged EXEC mode.

Release	Modification
12.2(19)S	This command was made available in user EXEC mode.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T. The **policy** keyword was added.
12.2(33)SRB	The **policy** keyword was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **show bgp all neighbors** command to display BGP and TCP connection information for neighbor sessions specific to address families such as IPv4, IPv6, Network Service Access Point (NSAP), Virtual Private Network (VPN) v4, and VPNv6.

Examples

The following example shows output of the **show bgp all neighbors** command:

```
Router# show bgp all neighbors

For address family: IPv4 Unicast
BGP neighbor is 172.16.232.53,  remote AS 100, external link
 Member of peer-group internal for session parameters
  BGP version 4, remote router ID 172.16.232.53
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        11
  Default minimum time between advertisement runs is 5 seconds

  Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 3FFE:700:20:1::12, Local port: 55345
Foreign host: 3FFE:700:20:1::11, Foreign port: 179

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x1A0D543C):
Timer          Starts    Wakeups            Next
Retrans          1218          5             0x0
TimeWait            0          0             0x0
AckHold          3327       3051             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
```

```
DeadWait            0          0             0x0

iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354     sndwnd:  15531
irs:  821333727  rcvnxt:  821591465  rcvwnd:      15547  delrcvwnd:    837

SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle

Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent: 4445 (retransmit: 5), with data: 4445, total data bytes: 244128

For address family: IPv6 Unicast

For address family: IPv4 MDT

For address family: VPNv4 Unicast

For address family: VPNv6 Unicast

For address family: IPv4 Multicast

For address family: IPv6 Multicast

For address family: NSAP Unicast
```

Table 10 describes the significant fields shown in the display.

Table 10 show bgp all neighbors Field Descriptions

Field	Description
For address family:	Address family to which the following fields refer.
BGP neighbor	IP address of the BGP neighbor and its autonomous system number.
remote AS	Autonomous system number of the neighbor.
external link	External Border Gateway Protocol (eBGP) peer.
BGP version	BGP version being used to communicate with the remote router.
remote router ID	IP address of the neighbor.
BGP state	State of this BGP connection.
up for	Time, in hh:mm:ss, that the underlying TCP connection has been in existence.
Last read	Time, in hh:mm:ss, since BGP last received a message from this neighbor.
hold time	Time, in seconds, that BGP will maintain the session with this neighbor without receiving messages.
keepalive interval	Time interval, in seconds, at which keepalive messages are transmitted to this neighbor.
Message statistics	Statistics organized by message type.
InQ depth is	Number of messages in the input queue.
OutQ depth is	Number of messages in the output queue.
Sent	Total number of transmitted messages.

Table 10 show bgp all neighbors Field Descriptions (continued)

Field	Description
Rcvd	Total number of received messages.
Opens	Number of open messages sent and received.
Notifications	Number of notification (error) messages sent and received.
Updates	Number of update messages sent and received.
Keepalives	Number of keepalive messages sent and received.
Route Refresh	Number of route refresh request messages sent and received.
Total	Total number of messages sent and received.
Default minimum time between...	Time, in seconds, between advertisement transmissions.
Connections established	Number of times a TCP and BGP connection has been successfully established.
dropped	Number of times that a valid session has failed or been taken down.
Last reset	Time, in hh:mm:ss, since this peering session was last reset. The reason for the reset is displayed on this line.
External BGP neighbor may be...	Indicates that the BGP Time-to-live (TTL) security check is enabled. The maximum number of hops that can separate the local and remote peer is displayed on this line.
Connection state	Connection status of the BGP peer.
Local host, Local port	IP address of the local BGP speaker and the port number.
Foreign host, Foreign port	Neighbor address and BGP destination port number.
Enqueued packets for retransmit:	Packets queued for retransmission by TCP.
Event Timers	TCP event timers. Counters are provided for starts and wakeups (expired timers).
Retrans	Number of times a packet has been retransmitted.
TimeWait	Time waiting for the retransmission timers to expire.
AckHold	Acknowledgment hold timer.
SendWnd	Transmission (send) window.
KeepAlive	Number of keepalive packets.
GiveUp	Number times a packet is dropped due to no acknowledgment.
PmtuAger	Path MTU discovery timer.
DeadWait	Expiration timer for dead segments.
iss:	Initial packet transmission sequence number.
snduna:	Last transmission sequence number that has not been acknowledged.
sndnxt:	Next packet sequence number to be transmitted.
sndwnd:	TCP window size of the remote host.
irs:	Initial packet receive sequence number.

Table 10 show bgp all neighbors Field Descriptions (continued)

Field	Description
rcvnxt:	Last receive sequence number that has been locally acknowledged.
rcvwnd:	TCP window size of the local host.
delrcvwnd:	Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT:	A calculated smoothed round-trip timeout.
RTTO:	Round-trip timeout.
RTV:	Variance of the round-trip time.
KRTT:	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.
minRTT:	Smallest recorded round-trip timeout (hard-wire value used for calculation).
maxRTT:	Largest recorded round-trip timeout.
ACK hold:	Length of time the local host will delay an acknowledgment to carry (piggyback) additional data.
IP Precedence value:	IP precedence of the BGP packets.
Datagrams	Number of update packets received from a neighbor.
Rcvd:	Number of received packets.
with data	Number of update packets sent with data.
total data bytes	Total amount of data received, in bytes.
Sent	Number of update packets sent.
with data	Number of update packets received with data.
total data bytes	Total amount of data sent, in bytes.

Related Commands

Command	Description
router bgp	Configures the BGP routing process.

show bgp nsap

To display entries in the Border Gateway Protocol (BGP) routing table for the network service access point (NSAP) address family, use the **show bgp nsap** command in EXEC mode.

show bgp nsap [*nsap-prefix*]

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast [*nsap-prefix*]

Syntax Description

unicast	Specifies NSAP unicast address prefixes.
nsap-prefix	(Optional) NSAP prefix number, entered to display a particular network in the BGP routing table for the NSAP address family. This argument may be any length up to 20 octets.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The **unicast** keyword was added and 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 **show bgp nsap** command provides output similar to the **show ip bgp** command, except that it is specific to the NSAP address family.

Examples

The following is sample output from the **show bgp nsap** command:

```
Router# show bgp nsap

BGP table version is 6, local router ID is 10.1.57.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 49.0101          49.0101.1111.1111.1111.1111.00
                                                       0 65101 i
* i49.0202.2222     49.0202.3333.3333.3333.3333.00
                                                100      0 ?
*>                  49.0202.2222.2222.2222.2222.00
                                                     32768 ?
* i49.0202.3333     49.0202.3333.3333.3333.3333.00
                                                100      0 ?
*>                  49.0202.2222.2222.2222.2222.00
                                                     32768 ?
```

```
*> 49.0303          49.0303.4444.4444.4444.4444.00
                                                        0 65303 i
*  49.0404          49.0303.4444.4444.4444.4444.00
                                                        0 65303 65404 i
*>i                 49.0404.9999.9999.9999.9999.00
                                              100       0 65404 i
```

Table 11 describes the significant fields shown in the display.

Table 11 show bgp nsap Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	NSAP prefix address of a network entity.
Next Hop	CLNS network entity title (NET) consisting of area address and system ID of the next system that is used when forwarding a packet to the destination network. This entry may cause a line break with the values of the following fields being displayed on the next line under their respective titles.
Metric	If shown, the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show bgp nsap** command, showing information for NSAP prefix 49.6005.1234.4567:

```
Router# show bgp nsap 49.6005.1234.4567

BGP routing table entry for 49.6005.1234.4567, version 2
Paths: (1 available, best #1)
  Not advertised to any peer
  Local
    49.6005.1234.4567.5678.1111.2222.3333.00 from 0.0.0.0 (10.1.1.1)
      Origin IGP, localpref 100, weight 32768, valid, sourced, local, best
```



Note If a prefix has not been advertised to any peer, the display shows “Not advertised to any peer.”

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast
```

show bgp nsap community

To display routes that belong to specified network service access point (NSAP) Border Gateway Protocol (BGP) communities, use the **show bgp nsap community** command in EXEC mode.

show bgp nsap community [*community-number*] [**exact-match** | **local-as** | **no-advertise** | **no-export**]

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast community [*community-number*] [**exact-match** | **local-as** | **no-advertise** | **no-export**]

Syntax Description

community-number	(Optional) Valid value is a community number in the range from 1 to 4294967295 or AA:NN (autonomous system-community number/2-byte number).
exact-match	(Optional) Displays only routes that have an exact match.
local-as	(Optional) Displays only routes that are not sent outside of the local autonomous system (well-known community).
no-advertise	(Optional) Displays only routes that are not advertised to any peer (well-known community).
no-export	(Optional) Displays only routes that are not exported outside of the local autonomous system (well-known community).
unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The **unicast** keyword was added and 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 **show bgp nsap community** command provides output similar to the **show ip bgp community** command, except that it is specific to the NSAP address family.

Communities are set with the **route-map** and **set community** commands. Communities are sent using the **neighbor send-community** and **neighbor route-map out** commands. You must enter the numerical communities before the well-known communities. For example, the following string does not work:

```
Router> show bgp nsap community local-as 111:12345
```

Use the following string instead:

```
Router> show bgp nsap community 111:12345 local-as
```

Examples

The following is sample output from the **show bgp nsap community** command:

```
Router# show bgp nsap community no-export

BGP table version is 5, local router ID is 10.1.57.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 49.0101.11       49.0101.2222.2222.2222.2222.00
                                                        0 101 i
```

Table 12 describes the significant fields shown in the display.

Table 12 show bgp nsap community Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	NSAP prefix address of a network entity.
Next Hop	CLNS network entity title (NET) consisting of area address and system ID of the next system that is used when forwarding a packet to the destination network. This entry may cause a line break with the values of the following fields being displayed on the next line under their respective titles.
Metric	If shown, the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast community no-export
```

Related Commands

Command	Description
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
set community	Sets the BGP communities attribute.
show bgp nsap community-list	Displays BGP community list information for the NSAP address family.

show bgp nsap community-list

To display routes that are permitted by the Border Gateway Protocol (BGP) community list for network service access point (NSAP) prefixes, use the **show bgp nsap community-list** command in EXEC mode.

show bgp nsap community-list *community-list-number* [**exact-match**]

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast community-list *community-list-number* [**exact-match**]

Syntax Description

community-list-number	Community list number in the range from 1 to 199.
exact-match	(Optional) Displays only routes that have an exact match.
unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The **unicast** keyword was added and 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 **show bgp nsap community-list** command provides output similar to the **show ip bgp community-list** command, except that it is specific to the NSAP address family.

Examples

The following is sample output of the **show bgp nsap community-list** command:

```
Router# show bgp nsap community-list 1

BGP table version is 6, local router ID is 10.0.22.33
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 49.0a0a.bb       49.0a0a.bbbb.bbbb.bbbb.bbbb.00
                                                          0 606
```

Table 13 describes the significant fields shown in the display.

Table 13 show bgp nsap community-list Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	NSAP prefix address of a network entity.
Next Hop	CLNS network entity title (NET) consisting of area address and system ID of the next system that is used when forwarding a packet to the destination network. This entry may cause a line break with the values of the following fields being displayed on the next line under their respective titles.
Metric	If shown, the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast community-list 1
```

show bgp nsap dampened-paths

Effective with Cisco IOS Release 12.2(33)SRB, the **show bgp nsap dampened-paths** command is replaced by the **show bgp nsap dampening** command. See the **show bgp nsap dampening** command for more information.

To display network service access point (NSAP) address family Border Gateway Protocol (BGP) dampened routes in the BGP routing table, use the **show bgp nsap dampened-paths** command in EXEC mode.

show bgp nsap dampened-paths

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	This command was replaced by the **show bgp nsap dampening** command in 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

In Cisco IOS Release 12.2(33)SRB and later releases, the **show bgp nsap dampened-paths** command is replaced by the **show bgp nsap dampening** command. A keyword, **dampened-paths**, can be used with the new **show bgp nsap dampened-paths** command to display NSAP address family BGP dampened routes.

Examples

The following is sample output from the **show bgp nsap dampened-paths** command in privileged EXEC mode:

```
Router# show bgp nsap dampened-paths

BGP table version is 20, local router ID is 10.1.57.13
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From             Reuse    Path
*d 49.0404          10.2.4.2         00:25:50 65202 65404 i
```

Table 14 describes the significant fields shown in the display.

Table 14 show bgp nsap dampened-paths Field Descriptions

Field	Description
BGP table version	Internal version number for the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.
*d	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear bgp nsap dampening	Clears BGP NSAP prefix route dampening information and unsuppresses the suppressed routes.

show bgp nsap dampening

To display network service access point (NSAP) address family Border Gateway Protocol (BGP) dampened routes in the BGP routing table, use the **show bgp nsap dampening** command in user EXEC or privileged EXEC mode.

show bgp nsap unicast dampening {**dampened-paths** | **flap-statistics** [**regexp** *regexp* | **quote-regexp** *regexp* | **filter-list** *access-list-number* | *nsap-prefix*] | **parameters**}

Syntax Description

unicast	Specifies NSAP unicast address prefixes.
dampened-paths	Displays paths suppressed due to dampening.
flap-statistics	Displays flap statistics of routes.
regexp *regexp*	(Optional) Displays flap statistics for all the paths that match the regular expression.
quote-regexp *regexp*	(Optional) Displays flap statistics for all the paths that match the regular expression as a quoted string of characters.
filter-list *access-list-number*	(Optional) Displays flap statistics for all the paths that pass the access list.
nsap-prefix	(Optional) Displays flap statistics for a single entry at this NSAP network number.
parameters	Displays details of configured dampening parameters.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Examples

The following is sample output from the **show bgp nsap dampened-paths** command in privileged EXEC mode:

```
Router# show bgp nsap unicast dampening dampened-paths

BGP table version is 20, local router ID is 10.1.57.13
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From            Reuse    Path
*d 49.0404          10.2.4.2        00:25:50 65202 65404 i
```

Table 14 describes the significant fields shown in the display.

Table 15 show bgp nsap unicast dampening dampened-paths Field Descriptions

Field	Description
BGP table version	Internal version number for the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

The following is sample output from the **show bgp nsap unicast dampening flap-statistics** command:

```
Router# show bgp nsap unicast dampening flap-statistics

BGP table version is 20, local router ID is 10.1.57.13
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From            Flaps Duration Reuse    Path
*d 49.0404          10.2.4.2        3     00:09:45 00:23:40 65202 65404
```

Table 16 describes the significant fields shown in the display.

Table 16 show bgp nsap unicast dampening flap-statistics Field Descriptions

Field	Description
BGP table version	Internal version number for the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.

Table 16 show bgp nsap unicast dampening flap-statistics Field Descriptions

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.
Flaps	Number of times the route has flapped.
Duration	Time (in hours:minutes:seconds) since the router noticed the first flap.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear bgp nsap dampening	Clears BGP NSAP prefix route dampening information and unsuppresses the suppressed routes.

show bgp nsap filter-list

To display routes in the Border Gateway Protocol (BGP) routing table for the network service access point (NSAP) address family that conform to a specified filter list, use the **show bgp nsap filter-list** command in privileged EXEC mode.

show bgp nsap filter-list *access-list-number*

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast filter-list *access-list-number*

Syntax Description

access-list-number	Number of an autonomous system path access list. It can be a number from 1 to 199.
unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The **unicast** keyword was added and 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.

Examples

The following is sample output from the **show bgp nsap filter-list** command:

```
Router# show bgp nsap filter-list 1

BGP table version is 3, local router ID is 10.0.11.33
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 49.0b0b          49.0b0b.bbbb.bbbb.bbbb.bbbb.00
                                                          0 707 i
```

Table 17 describes the significant fields shown in the display.

Table 17 show bgp nsap filter-list Field Descriptions

Field	Description
BGP table version	Internal version number for the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Table 17 show bgp nsap filter-list Field Descriptions (continued)

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	NSAP prefix address of a network entity.
Next Hop	CLNS network entity title (NET) consisting of area address and system ID of the next system that is used when forwarding a packet to the destination network. This entry may cause a line break with the values of the following fields being displayed on the next line under their respective titles.
Metric	If shown, the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Set through the use of autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast filter-list 1
```

show bgp nsap flap-statistics

To display Border Gateway Protocol (BGP) flap statistics for network service access point (NSAP) prefixes, use the **show bgp nsap flap-statistics** command in EXEC mode.

show bgp nsap flap-statistics [**regexp** *regexp* | **quote-regexp** *regexp* | **filter-list** *access-list-number* | *nsap-prefix*]

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast flap-statistics [**regexp** *regexp* | **quote-regexp** *regexp* | **filter-list** *access-list-number* | *nsap-prefix*]

Syntax Description

regexp *regexp*	(Optional) Displays flap statistics for all the paths that match the regular expression.
quote-regexp *regexp*	(Optional) Displays flap statistics for all the paths that match the regular expression as a quoted string of characters.
filter-list *access-list-number*	(Optional) Displays flap statistics for all the paths that pass the access list.
nsap-prefix	(Optional) Displays flap statistics for a single entry at this NSAP network number.
unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The **unicast** keyword was added and 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 **show bgp nsap flap-statistics** command provides output similar to the **show ip bgp flap-statistics** command, except that it is specific to the NSAP address family.

If no arguments or keywords are specified, the router displays flap statistics for all NSAP prefix routes.

Examples

The following is sample output from the **show bgp nsap flap-statistics** command without arguments or keywords:

```
Router# show bgp nsap flap-statistics

BGP table version is 20, local router ID is 10.1.57.13
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
   Network          From            Flaps Duration Reuse    Path
*d 49.0404          10.2.4.2        3     00:09:45 00:23:40 65202 65404
```

Table 18 describes the significant fields shown in the display.

Table 18 show bgp nsap flap-statistics Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.
Flaps	Number of times the route has flapped.
Duration	Time (in hours:minutes:seconds) since the router noticed the first flap.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	AS-path of the route that is being dampened.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast flap-statistics
```

Related Commands

Command	Description

bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear bgp nsap flap-statistics	Clears BGP flap statistics for NSAP prefix routes.

show bgp nsap inconsistent-as

To display Border Gateway Protocol (BGP) network service access point (NSAP) prefix routes with inconsistent originating autonomous systems, use the **show bgp nsap inconsistent-as** command in EXEC mode.

show bgp nsap inconsistent-as

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast inconsistent-as

Syntax Description

unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The **unicast** keyword was added and 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 **show bgp nsap inconsistent-as** command provides output similar to the **show ip bgp inconsistent-as** command, except that it is specific to the NSAP address family.

Use the **show bgp nsap inconsistent-as** command to discover any BGP routing table entries that contain inconsistent autonomous system path information. Inconsistent autonomous path information is useful for troubleshooting networks because it highlights a configuration error in the network.

Examples

The following is sample output from the **show bgp nsap inconsistent-as** command. In this example, the network prefix of 49.0a0a has two entries in the BGP routing table showing different originating paths. The originating path information should be the same in both entries.

```
Router# show bgp nsap inconsistent-as

BGP table version is 3, local router ID is 10.1.57.17
Status codes: s suppressed, d damped, h history, * valid, > best, i -internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  49.0a0a          49.0a0a.cccc.cccc.cccc.00
                                                          0 30 i
*>                  49.0a0a.aaaa.aaaa.aaaa.00
                                                          0 10 i
```

Table 19 describes the significant fields shown in the display.

Table 19 show bgp nsap inconsistent-as Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	NSAP prefix address of a network entity.
Next Hop	CLNS network entity title (NET) consisting of area address and system ID of the next system that is used when forwarding a packet to the destination network. This entry may cause a line break with the values of the following fields being displayed on the next line under their respective titles.
Metric	If shown, the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast inconsistent-as
```

show bgp nsap neighbors

To display information about Border Gateway Protocol (BGP) network service access point (NSAP) prefix connections to neighbors, use the **show bgp nsap neighbors** command in EXEC mode.

show bgp nsap neighbors [*ip-address* [**routes** | **flap-statistics** | **advertised-routes** | **paths** *regexp* | **dampened-routes**]]

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast neighbors [*ip-address* [**routes** | **flap-statistics** | **advertised-routes** | **paths** *regexp* | **dampened-routes**]]

Syntax Description

ip-address	(Optional) IP address of the BGP-speaking neighbor. If you omit this argument, all neighbors are displayed.
routes	(Optional) Displays all routes received and accepted.
flap-statistics	(Optional) Displays flap statistics for the routes learned from the neighbor.
advertised-routes	(Optional) Displays all the routes the networking device advertised to the neighbor.
paths *regexp*	(Optional) Regular expression used to match the paths received.
dampened-routes	(Optional) Displays the dampened routes to the neighbor at the NSAP prefix address specified.
unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The **unicast** keyword was added and 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 **show bgp nsap neighbors** command provides output similar to the **show ip bgp neighbors** command, except that it is specific to the NSAP address family.

Examples

The following is sample output from the **show bgp nsap neighbors** command:

```
Router# show bgp nsap neighbors 10.0.2.3

BGP neighbor is 10.0.2.3,  remote AS 64500, external link
  BGP version 4, remote router ID 172.17.1.2
  BGP state = Established, up for 00:12:50
  Last read 00:00:50, hold time is 180, keepalive interval is 60 seconds
```

```
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family NSAP Unicast: advertised and received
  Received 17 messages, 0 notifications, 0 in queue
  Sent 17 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Default minimum time between advertisement runs is 30 seconds

 For address family: NSAP Unicast
  BGP table version 5, neighbor version 5
  Index 2, Offset 0, Mask 0x4
  2 accepted prefixes consume 114 bytes
  Prefix advertised 2, suppressed 0, withdrawn 0
  Number of NLRIs in the update sent: max 1, min 0

  Connections established 1; dropped 0
  Last reset never
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 10.0.2.2, Local port: 11000
Foreign host: 10.0.2.3, Foreign port: 179

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x115940):
Timer          Starts    Wakeups            Next
Retrans            22          1             0x0
TimeWait            0          0             0x0
AckHold            19          7             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 2052706884  snduna: 2052707371  sndnxt: 2052707371     sndwnd:  15898
irs: 1625021348  rcvnxt: 1625021835  rcvwnd:      15898  delrcvwnd:    486

SRTT: 279 ms, RTTO: 446 ms, RTV: 167 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle

Datagrams (max data segment is 1460 bytes):
Rcvd: 30 (out of order: 0), with data: 19, total data bytes: 486
Sent: 29 (retransmit: 1, fastretransmit: 0), with data: 20, total data bytes: 46
```

Table 20 describes the significant fields shown in the display.

Table 20 show bgp nsap neighbors Field Descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number.
remote AS	Autonomous system of the neighbor.
link	If the neighbor is in the same autonomous system as the router, then the link between them is internal; otherwise, it is considered external.
BGP version	BGP version being used to communicate with the remote router; the router ID (an IP address) of the neighbor is also specified.
remote router ID	A 32-bit number written as 4 octets separated by periods (dotted decimal format).

Table 20 show bgp nsap neighbors Field Descriptions (continued)

Field	Description
BGP state	Internal state of this BGP connection.
up for	Amount of time (in hours:minutes:seconds) that the underlying TCP connection has been in existence.
Last read	Time (in hours:minutes:seconds) that BGP last read a message from this neighbor.
hold time	Maximum amount of time, in seconds, that can elapse between messages from the peer.
keepalive interval	Time period, in seconds, between sending keepalive packets, which help ensure that the TCP connection is up.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor.
Route refresh	Indicates that the neighbor supports dynamic soft reset using the route refresh capability.
Address family NSAP Unicast	NSAP unicast-specific properties of this neighbor.
Received	Number of total BGP messages received from this peer, including keepalives.
notifications	Number of error messages received from the peer.
Sent	Total number of BGP messages that have been sent to this peer, including keepalives.
notifications	Number of error messages the router has sent to this peer.
Route refresh request	Number of route refresh requests sent and received from this neighbor.
advertisement runs	Value of minimum advertisement interval.
For address family	Address family to which the following fields refer.
BGP table version	Indicates that the neighbor has been updated with this version of the primary BGP routing table.
neighbor version	Number used by the software to track the prefixes that have been sent and those that must be sent to this neighbor.
Community attribute (not shown in sample output)	Appears if the **neighbor send-community** command is configured for this neighbor.
Inbound path policy (not shown in sample output)	Indicates that an inbound filter list or route map is configured.
Outbound path policy (not shown in sample output)	Indicates that an outbound filter list, route map, or unsuppress map is configured.
bgp-in (not shown in sample output)	Name of the inbound update prefix filter list for the NSAP unicast address family.
aggregate (not shown in sample output)	Name of the outbound update prefix filter list for the NSAP unicast address family.
uni-out (not shown in sample output)	Name of the outbound route map for the NSAP unicast address family.

Table 20 show bgp nsap neighbors Field Descriptions (continued)

Field	Description
accepted prefixes	Number of prefixes accepted.
Prefix advertised	Number of prefixes advertised.
suppressed	Number of prefixes suppressed.
withdrawn	Number of prefixes withdrawn.
history paths (not shown in sample output)	Number of path entries held to remember history.
Connections established	Number of times the router has established a TCP connection and the two peers have agreed to speak BGP with each other.
dropped	Number of times that a good connection has failed or been taken down.
Last reset	Elapsed time since this peering session was last reset.
Connection state	State of the BGP peer.
unread input bytes	Number of bytes of packets still to be processed.
Local host, Local port	Peering address of local router, plus port.
Foreign host, Foreign port	Peering address of the neighbor.
Event Timers	Table that displays the number of starts and wakeups for each timer.
iss	Initial send sequence number.
snduna	Last send sequence number the local host sent but for which it has not received an acknowledgment.
sndnxt	Sequence number the local host will send next.
sndwnd	TCP window size of the remote host.
irs	Initial receive sequence number.
rcvnxt	Last receive sequence number the local host has acknowledged.
rcvwnd	TCP window size of the local host.
delrcvwnd	Delayed receive window—data the local host has read from the connection but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT	A calculated smoothed round-trip timeout.
RTTO	Round-trip timeout.
RTV	Variance of the round-trip time.
KRTT	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.
minRTT	Smallest recorded round-trip timeout (hard wire value used for calculation).
maxRTT	Largest recorded round-trip timeout.
ACK hold	Time (in milliseconds) the local host will delay an acknowledgment in order to “piggyback” data on it.
Flags	IP precedence of the BGP packets.

Table 20 show bgp nsap neighbors Field Descriptions (continued)

Field	Description
Datagrams: Rcvd	Number of update packets received from neighbor.
with data	Number of update packets received with data.
total data bytes	Total bytes of data.
Sent	Number of update packets sent.
with data	Number of update packets with data sent.
total data bytes	Total number of data bytes.

The following is sample output from the **show bgp nsap neighbors** command with the **advertised-routes** keyword:

```
Router# show bgp nsap neighbors 10.0.2.3 advertised-routes

BGP table version is 5, local router ID is 172.17.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 49.0101          49.0101.1111.1111.1111.1111.00
                                                          0 101 i
*> 49.0202          49.0202.2222.2222.2222.2222.00
                                                          32768 i
```

The following is sample output from the **show bgp nsap neighbors** command with the **routes** keyword:

```
Router# show bgp nsap neighbors 10.0.2.3 routes

BGP table version is 5, local router ID is 172.17.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 49.0303          49.0303.3333.3333.3333.3333.00
                                                        0 303 i
*> 49.0404          49.0303.3333.3333.3333.3333.00
                                                        0 303 404 i

Total number of prefixes 2
```

Table 21 describes the significant fields shown in the display.

Table 21 show bgp nsap neighbors Field Descriptions with advertised-routes and routes keywords

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Table 21 show bgp nsap neighbors Field Descriptions with advertised-routes and routes keywords (continued)

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	NSAP prefix address of a network entity.
Next Hop	CLNS network entity title (NET) consisting of area address and system ID of the next system that is used when forwarding a packet to the destination network. This entry may cause a line break with the values of the following fields being displayed on the next line under their respective titles.
Metric	If shown, the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show bgp nsap neighbors** command with the **paths** keyword:

```
Router# show bgp nsap neighbors 10.0.3.3 paths ^101

Address    Refcount Metric Path
0x62281590        1      0 101 i
```

Note The caret (^) symbol in the example is a regular expression that is entered by simultaneously pressing the Shift and 6 keys on your keyboard. A caret (^) symbol at the beginning of a regular expression matches the start of a line.

Table 22 describes the significant fields shown in the display.

Table 22 show bgp nsap neighbors paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Refcount	Number of routes using that path.
Metric	The Multiple Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The AS-path for that route, followed by the origin code for that route.

The following sample output from the **show bgp nsap neighbors** command shows the NSAP prefix dampened routes for the neighbor at 10.0.2.2:

```
Router# show bgp nsap neighbors 10.0.2.2 dampened-routes

BGP table version is 10, local router ID is 172.17.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From             Reuse    Path
*d 49.0101          10.0.2.2         00:25:50 202 101 i
```

The following sample output from the **show bgp nsap neighbors** command shows the NSAP prefix flap statistics for the neighbor at 10.0.2.2:

```
Router# show bgp nsap neighbors 10.0.2.2 flap-statistics

BGP table version is 10, local router ID is 10.1.57.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From            Flaps Duration Reuse    Path
*d 49.0101          10.0.2.2        3     00:07:00 00:24:50 202 101
```

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast neighbors 10.0.2.3
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a neighboring router.

show bgp nsap paths

To display all the Border Gateway Protocol (BGP) network service access point (NSAP) prefix paths in the database, use the **show bgp nsap paths** command in EXEC mode.

show bgp nsap paths [*AS-path-regexp*]

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast paths [*AS-path-regexp*]

Syntax Description

AS-path-regexp	(Optional) Regular expression that is used to match the received paths in the database.
unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The **unicast** keyword was added and 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 **show bgp nsap paths** command provides output similar to the **show ip bgp paths** command, except that it is specific to the NSAP address family.

Examples

The following is sample output from the **show bgp nsap paths** command without a specified regular expression:

```
Router# show bgp nsap paths

Address    Hash Refcount Metric Path
0x622803FC    0        1      0 i
0x62280364 1197        1      0 202 101 i
0x62280448 1739        1      0 202 i
0x622803B0 1941        1      0 404 i
```

Table 23 describes the significant fields shown in the display.

Table 23 show bgp nsap paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Hash	Hash bucket where the path is stored.

Table 23 show bgp nsap paths Field Descriptions (continued)

Field	Description
Refcount	Number of routes using that path.
Metric	The Multiple Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The AS-path for that route, followed by the origin code for that route.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast paths
```

show bgp nsap quote-regexp

To display Border Gateway Protocol (BGP) network service access point (NSAP) prefix routes matching the AS-path regular expression as a quoted string of characters, use the **show bgp nsap quote-regexp** command in privileged EXEC mode.

show bgp nsap quote-regexp *as-path-regexp*

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast quote-regexp *as-path-regexp*

Syntax Description

as-path-regexp	Regular expression to match the BGP autonomous system paths. The regular expression is contained within quotes.
unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The **unicast** keyword was added and 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 **show bgp nsap quote-regexp** command provides output similar to the **show ip bgp quote-regexp** command, except that it is specific to the NSAP address family.

Examples

The following is sample output from the **show bgp nsap quote-regexp** command that shows paths equal to 202:

```
Router# show bgp nsap quote-regexp "202"

BGP table version is 10, local router ID is 10.1.57.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*d 49.0101          49.0202.2222.2222.2222.2222.00
                                                          0 202 101 i
*> 49.0202          49.0202.2222.2222.2222.2222.00
                                                          0 202 i
```

Table 24 describes the significant fields shown in the display.

Table 24 show bgp nsap quote-regexp Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	NSAP prefix of a network entity.
Next Hop	CLNS network entity title (NET) consisting of area address and system ID of the next system that is used when forwarding a packet to the destination network. This entry may cause a line break with the values of the following fields being displayed on the next line under their respective titles.
Metric	If shown, the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast quote-regexp "202"
```

Related Commands

Command	Description
show bgp nsap regexp	Displays NSAP prefix routes matching the AS-path regular expression.

show bgp nsap regexp

To display Border Gateway Protocol (BGP) network service access point (NSAP) prefix routes matching the AS-path regular expression, use the **show bgp nsap regexp** command in privileged EXEC mode.

show bgp nsap regexp *AS-path-regexp*

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast regexp *AS-path-regexp*

Syntax Description

AS-path-regexp	Regular expression to match the BGP autonomous system paths.
unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The **unicast** keyword was added and 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 **show bgp nsap regexp** command provides output similar to the **show ip bgp regexp** command, except that it is specific to the NSAP address family.

Examples

The following is sample output from the **show bgp nsap regexp** command that shows paths beginning with 202 or containing 101:

```
Router# show bgp nsap regexp ^202 101

BGP table version is 10, local router ID is 10.1.57.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*d 49.0101          49.0202.2222.2222.2222.2222.00
                                                          0 202 101 i
```

Note The caret (^) symbol in the example is a regular expression that is entered by simultaneously pressing the Shift and 6 keys on your keyboard. A caret (^) symbol at the beginning of a regular expression matches the start of a line.

Table 25 describes the significant fields shown in the display.

Table 25 show bgp nsap regexp Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	NSAP prefix address of a network entity.
Next Hop	CLNS network entity title (NET) consisting of area address and system ID of the next system that is used when forwarding a packet to the destination network. This entry may cause a line break with the values of the following fields being displayed on the next line under their respective titles.
Metric	If shown, the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast regexp ^202 101
```

Related Commands

Command	Description
show bgp nsap quote-regexp	Displays BGP NSAP prefix routes matching the AS-path regular expression.

show bgp nsap summary

To display the status of all Border Gateway Protocol (BGP) network service access point (NSAP) prefix connections, use the **show bgp nsap summary** command in EXEC mode.

show bgp nsap summary

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast summary

Syntax Description

unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The **unicast** keyword was added and 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 **show bgp nsap summary** command provides output similar to the **show ip bgp summary** command, except that it is specific to the NSAP address family.

Examples

The following is sample output from the **show bgp nsap summary** command:

```
Router# show bgp nsap summary

BGP router identifier 10.2.4.2, local AS number 65202
BGP table version is 26, main routing table version 26
5 network entries and 8 paths using 1141 bytes of memory
6 BGP path attribute entries using 360 bytes of memory
4 BGP AS-PATH entries using 96 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Dampening enabled. 0 history paths, 0 dampened paths
BGP activity 16/261 prefixes, 34/26 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.2.1        4 65101    1162    1162       26    0    0 18:17:07        1
10.2.3.3        4 65202    1183    1188       26    0    0 18:23:28        3
10.2.4.4        4 65303    1163    1187       26    0    0 18:23:14        2
```

Table 26 describes the significant fields shown in the display.

Table 26 show bgp nsap summary Field Descriptions

Field	Description
BGP router identifier	IP address of the networking device.
local AS number	Number of the local autonomous system.
BGP table version	Internal version number of the BGP database.
main routing table version	Last version of the BGP database that was injected into the main routing table.
network entries	Number of network entries and paths in the main routing table including the associated memory usage.
BGP path attribute entries	Number of BGP path attribute entries in the main routing table including the associated memory usage.
BGP route-map cache entries	Number of BGP route map cache entries in the main routing table including the associated memory usage.
BGP filter-list cache entries	Number of BGP filter list cache entries in the main routing table including the associated memory usage.
Dampening	Indicates whether route dampening is enabled, the number of history paths, and number of dampened paths.
BGP activity	Displays the number of BGP prefixes and paths, followed by the BGP scan interval in seconds.
Neighbor	IP address of a neighbor.
V	BGP version number communicated to that neighbor.
AS	Autonomous system.
MsgRcvd	BGP messages received from that neighbor.
MsgSent	BGP messages sent to that neighbor.
TblVer	Last version of the BGP database that was sent to that neighbor.
InQ	Number of messages from that neighbor waiting to be processed.
OutQ	Number of messages waiting to be sent to that neighbor.
Up/Down	The length of time that the BGP session has been in state Established, or the current state if it is not Established.
State/PfxRcd	Current state of the BGP session/the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the **neighbor maximum-prefix** command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the **neighbor shutdown** command.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast summary
```

Related Commands

Command	Description
clear bgp nsap	Resets an NSAP BGP TCP connection.
neighbor maximum-prefix	Controls how many prefixes can be received from a neighbor.
neighbor shutdown	Disables a neighbor or peer group.

show ip as-path-access-list

To display the contents of all current autonomous system (AS) path access lists, use the **show ip as-path-access-list** command in user EXEC or privileged EXEC mode.

show ip as-path-access-list [*number*]

Syntax Description

number	(Optional) Specifies the AS path access list number. The range is from 1 to 500.

Command Default

If the *number* argument is not specified, command output is displayed for all AS path access lists.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following is sample output from the **show ip as-path-access-list** command:

```
Router# show ip as-path-access-list

AS path access list 34
    deny RTR$
AS path access list 100
    permit 100$
```

Table 27 describes the fields shown in the display.

Table 27 show ip as-path-access-list Field Descriptions

Field	Description
AS path access list	Indicates the AS path access list number.
deny	Indicates the number of packets that are rejected since the regular expression failed to match the representation of the AS path of the route as an ASCII string.
permit	Indicates the number of packets that are forwarded since the regular expression matched the representation of the AS path of the route as an ASCII string.

Related Commands

Command	Description
ip as-path access-list	Configures an autonomous system path filter using a regular expression.

show ip bgp

To display entries in the Border Gateway Protocol (BGP) routing table, use the **show ip bgp** command in user EXEC or privileged EXEC mode.

show ip bgp [*ip-address* [*mask* [**longer-prefixes** [**injected**] | **shorter-prefixes** [*length*] | **bestpath** | **multipaths** | **subnets**] | **bestpath** | **multipaths**] | **all** | **oer-paths** | **prefix-list** *name* | **pending-prefixes** | **route-map** *name*]

Syntax Description

ip-address	(Optional) IP address entered to filter the output to display only a particular host or network in the BGP routing table.
mask	(Optional) Mask to filter or match hosts that are part of the specified network.
longer-prefixes	(Optional) Displays the specified route and all more specific routes.
injected	(Optional) Displays more specific prefixes injected into the BGP routing table.
shorter-prefix	(Optional) Displays the specified route and all less specific routes.
length	(Optional) The prefix length. The value for this argument is a number from 0 to 32.
bestpath	(Optional) Displays the bestpath for this prefix
multipaths	(Optional) Displays multipaths for this prefix.
subnets	(Optional) Displays the subnet routes for the specified prefix.
all	(Optional) Displays all address family information in the BGP routing table.
oer-paths	(Optional) Displays Optimized Edge Routing (OER) controlled prefixes in the BGP routing table.
prefix-list *name*	(Optional) Filters the output based on the specified prefix list.
pending-prefixes	(Optional) Displays prefixes that are pending deletion from the BGP routing table.
route-map *name*	(Optional) Filters the output based on the specified route map.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0	This command was modified. The display of prefix advertisement statistics was added.
12.0(6)T	This command was modified. The display of a message indicating support for route refresh capability was added.
12.0(14)ST	This command was modified. The **prefix-list**, **route-map**, and **shorter-prefixes** keywords were added.
12.2(2)T	This command was modified. The output was modified to display multipaths and a best path to the specified network.

Release	Modification
12.0(21)ST	The output was modified to show the number of Multiprotocol Label Switching (MPLS) labels that arrive at and depart from the prefix.
12.0(22)S	This command was modified. A new status code indicating stale routes was added to support BGP graceful restart.
12.2(14)S	This command was modified. A message indicating support for BGP policy accounting was added and this command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(15)T	This command was modified. A new status code indicating stale routes was added to support BGP graceful restart.
12.3(2)T	This command was modified. The **all** keyword was added.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.3(8)T	This command was modified. The **oer-paths** keyword was added.
12.4(15)T	This command was modified. The **pending-prefixes**, **bestpath**, **multipaths**, and **subnets** keywords were 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.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
12.2(33)SRE	This command was modified. The command output was modified to show the backup path and the best external path information. Support for the best external route and backup path was added. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

The **show ip bgp** command is used to display the contents of the BGP routing table. The output can be filtered to display entries for a specific prefix, prefix length, and prefixes injected through a prefix list, route map, or conditional advertisement.

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.

oer-paths Keyword

In Cisco IOS Release 12.3(8)T, and later releases, BGP prefixes that are monitored and controlled by OER are displayed by entering the **show ip bgp** command with the **oer-paths** keyword.

Examples

- **show ip bgp: Example, page 442**
- **show ip bgp (4-Byte Autonomous System Numbers): Example, page 444**
- **show ip bgp ip-address: Example, page 444**
- **show ip bgp all: Example, page 445**
- **show ip bgp longer-prefixes: Example, page 447**
- **show ip bgp shorter-prefixes: Example, page 447**
- **show ip bgp prefix-list: Example, page 447**
- **show ip bgp route-map: Example, page 448**

show ip bgp: Example

The following sample output shows the BGP routing table:

```
Router# show ip bgp

BGP table version is 22, local router ID is 10.1.1.1
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
*> 10.1.1.1/32      0.0.0.0                  0         32768 i
*>i10.2.2.2/32      172.16.1.2               0    100      0 i
*bi10.9.9.9/32      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
* i172.16.1.0/24    172.16.1.2               0    100      0 i
*>                  0.0.0.0                  0         32768 i
*> 192.168.1.0      0.0.0.0                  0         32768 i
*>i192.168.3.0      172.16.1.2               0    100      0 i
*bi192.168.9.0      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
*bi192.168.13.0     192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
```

Table 28 describes the significant fields shown in the display.

Table 28 show ip bgp Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session. • r—The table entry is a RIB-failure. • S—The table entry is stale. • m—The table entry has multipath to use for that network. • b—The table entry has backup path to use for that network. • x—The table entry has best external route to use for the network.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from an Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.
(stale)	Indicates that the following path for the specified autonomous system is marked as “stale” during a graceful restart process.

show ip bgp (4-Byte Autonomous System Numbers): Example

The following sample output shows the BGP routing table with 4-byte autonomous system numbers, 65536 and 65550, shown under the Path field. 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.

```
RouterB# show ip bgp

BGP table version is 4, 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 65536  i
*> 10.2.2.0/24      192.168.3.2              0             0 65550  i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i
```

show ip bgp ip-address: Example

The following sample output displays information about the 192.168.1.0 entry in the BGP routing table:

```
Router# show ip bgp 192.168.1.0

BGP routing table entry for 192.168.1.0/24, version 22
Paths: (2 available, best #2, table default)
  Additional-path
  Advertised to update-groups:
     3
  10 10
    192.168.3.2 from 172.16.1.2 (10.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
  10 10
    192.168.1.2 from 192.168.1.2 (10.3.3.3)
      Origin IGP, localpref 100, valid, external, best , recursive-via-connected
```

The following sample output displays information about the 10.3.3.3 255.255.255.255 entry in the BGP routing table:

```
Router# show ip bgp 10.3.3.3 255.255.255.255

BGP routing table entry for 10.3.3.3/32, version 35
Paths: (3 available, best #2, table default)
Multipath: eBGP
Flag: 0x860
  Advertised to update-groups:
     1
  200
    10.71.8.165 from 10.71.8.165 (192.168.0.102)
      Origin incomplete, localpref 100, valid, external, backup/repair
      Only allowed to recurse through connected route
  200
    10.71.11.165 from 10.71.11.165 (192.168.0.102)
      Origin incomplete, localpref 100, weight 100, valid, external, best
      Only allowed to recurse through connected route
  200
    10.71.10.165 from 10.71.10.165 (192.168.0.104)
      Origin incomplete, localpref 100, valid, external,
      Only allowed to recurse through connected route
```

Table 29 describes the significant fields shown in the display.

Table 29 show ip bgp Field Descriptions

Field	Description
BGP routing table entry for	IP address or network number of the routing table entry.
version	Internal version number of the table. This number is incremented whenever the table changes.
Paths	The number of available paths, and the number of installed best paths. This line displays “Default-IP-Routing-Table” when the best path is installed in the IP routing table.
Multipath	This field is displayed when multipath loadsharing is enabled. This field will indicate if the multipaths are iBGP or eBGP.
Advertised to update-groups	The number of each update group for which advertisements are processed.
Origin	Origin of the entry. The origin can be IGP, EGP, or incomplete. This line displays the configured metric (0 if no metric is configured), the local preference value (100 is default), and the status and type of route (internal, external, multipath, best).
Extended Community	This field is displayed if the route carries an extended community attribute. The attribute code is displayed on this line. Information about the extended community is displayed on a subsequent line.

show ip bgp all: Example

The following is sample output from the **show ip bgp** command entered with the **all** keyword. Information about all configured address families is displayed.

```
Router# show ip bgp all

For address family: IPv4 Unicast   *****
BGP table version is 27, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                  0         32768 ?
*> 10.13.13.0/24    0.0.0.0                  0         32768 ?
*> 10.15.15.0/24    0.0.0.0                  0         32768 ?
*>i10.18.18.0/24    172.16.14.105         1388  91351      0 100 e
*>i10.100.0.0/16    172.16.14.107          262    272      0 1 2 3 i
*>i10.100.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.101.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.103.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.104.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.100.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*>i10.101.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*  10.100.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*  10.101.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*> 10.102.0.0/16    172.16.14.108         1388             0 100 e
*> 172.16.14.0/24   0.0.0.0                  0         32768 ?
*> 192.168.5.0      0.0.0.0                  0         32768 ?
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
```

```
For address family: VPNv4 Unicast   *****
BGP table version is 21, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf vpn1)
*> 10.1.1.0/24      192.168.4.3           1622             0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.2.0/24      192.168.4.3           1622             0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.3.0/24      192.168.4.3           1622             0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.4.0/24      192.168.4.3           1622             0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.5.0/24      192.168.4.3           1622             0 100 53285 33299 51178
{27016,57039,16690} e
*>i172.17.1.0/24    10.3.3.3                 10     30      0 53285 33299 51178 47751 ?
*>i172.17.2.0/24    10.3.3.3                 10     30      0 53285 33299 51178 47751 ?
*>i172.17.3.0/24    10.3.3.3                 10     30      0 53285 33299 51178 47751 ?
*>i172.17.4.0/24    10.3.3.3                 10     30      0 53285 33299 51178 47751 ?
*>i172.17.5.0/24    10.3.3.3                 10     30      0 53285 33299 51178 47751 ?

For address family: IPv4 Multicast   *****
BGP table version is 11, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.40.40.0/26    172.16.14.110        2219             0 21 22 {51178,47751,27016} e
*                   10.1.1.1              1622             0 15 20 1 {2} e
*> 10.40.40.64/26   172.16.14.110        2219             0 21 22 {51178,47751,27016} e
*                   10.1.1.1              1622             0 15 20 1 {2} e
*> 10.40.40.128/26  172.16.14.110        2219             0 21 22 {51178,47751,27016} e
*                   10.1.1.1              2563             0 15 20 1 {2} e
*> 10.40.40.192/26  10.1.1.1              2563             0 15 20 1 {2} e
*> 10.40.41.0/26    10.1.1.1              1209             0 15 20 1 {2} e
*>i10.102.0.0/16    10.1.1.1               300    500      0 5 4 {101,102} e
*>i10.103.0.0/16    10.1.1.1               300    500      0 5 4 {101,102} e

For address family: NSAP Unicast *****
BGP table version is 1, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* i45.0000.0002.0001.000c.00
                    49.0001.0000.0000.0a00
                                                100      0 ?
* i46.0001.0000.0000.0000.0a00
                    49.0001.0000.0000.0a00
                                                100      0 ?
* i47.0001.0000.0000.000b.00
                    49.0001.0000.0000.0a00
                                                100      0 ?
* i47.0001.0000.0000.000e.00
                    49.0001.0000.0000.0a00
```

show ip bgp longer-prefixes: Example

The following is sample output from the **show ip bgp** command entered with the **longer-prefixes** keyword:

```
Router# show ip bgp 10.92.0.0 255.255.0.0 longer-prefixes

BGP table version is 1738, local router ID is 192.168.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 10.92.0.0         10.92.72.30        8896         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.1.0         10.92.72.30        8796         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.11.0        10.92.72.30       42482         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.14.0        10.92.72.30        8796         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.15.0        10.92.72.30        8696         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.16.0        10.92.72.30        1400         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.17.0        10.92.72.30        1400         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.18.0        10.92.72.30        8876         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.19.0        10.92.72.30        8876         32768 ?
*                    10.92.72.30                         0 109 108 ?
```

show ip bgp shorter-prefixes: Example

The following is sample output from the **show ip bgp** command entered with the **shorter-prefixes** keyword. An 8-bit prefix length is specified.

```
Router# show ip bgp 172.16.0.0/16 shorter-prefixes 8

*> 172.16.0.0         10.0.0.2                              0 ?
*                     10.0.0.2                0             0 200 ?
```

show ip bgp prefix-list: Example

The following is sample output from the **show ip bgp** command entered with the **prefix-list** keyword:

```
Router# show ip bgp prefix-list ROUTE

BGP table version is 39, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                               0 ?
*                   10.0.0.2                 0             0 200 ?
```

show ip bgp route-map: Example

The following is sample output from the **show ip bgp** command entered with the **route-map** keyword:

```
Router# show ip bgp route-map LEARNED_PATH

BGP table version is 40, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                             0 ?
*                   10.0.0.2                  0          0 200 ?
```

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.
ip prefix-list	Creates a prefix list or adds a prefix-list entry.
route-map	Defines the conditions for redistributing routes from one routing protocol into another routing protocol.
router bgp	Configures the BGP routing process.

show ip bgp all dampening

To display BGP dampening information, use the **show ip bgp all dampening** command in user EXEC or privileged EXEC mode.

show ip bgp all dampening {**dampened-paths** | **flap-statistics** [**filter-list** *filter-list* | **quote-regexp** *regexp* | **regexp** *regexp*] | **parameters**}

Syntax Description

dampened-paths	Display routes suppressed due to dampening.
flap-statistics	Displays flap statistics of routes.
filter-list *filter-list*	(Optional) Used with the **flap-statistics** keyword, displays routes that conform to the specified filter list in the range 1-500.
quote-regexp *regexp*	(Optional) Used with the **flap-statistics** keyword, displays routes matching the AS path "regular expression".
regexp *regexp*	(Optional) Used with the **flap-statistics** keyword, displays routes matching the AS path regular expression.
parameters	Display details of configured dampening parameters.

Command Modes

User EXEC (>)
Privileged EXEC

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use this command to display BGP dampening information.

Examples

The following example show how to display the BGP dampening parameters.

```
Router# show ip bgp all dampening parameters
For address family: IPv4 Unicast

% dampening not enabled for base

For address family: VPNv4 Unicast

% dampening not enabled for base

For vrf: Cust_A
 dampening 15 750 2000 60 (DEFAULT)
  Half-life time      : 15 mins       Decay Time       : 2320 secs
  Max suppress penalty: 12000         Max suppress time: 60 mins
  Suppress penalty    :  2000         Reuse penalty    : 750


For vrf: Cust_B

 dampening 15 750 2000 60 (DEFAULT)
```

```
  Half-life time      : 15 mins       Decay Time       : 2320 secs
  Max suppress penalty: 12000         Max suppress time: 60 mins
  Suppress penalty    :  2000         Reuse penalty    : 750


For address family: IPv4 Multicast

% dampening not enabled for base
Router#
```

Table 30 describes the significant fields shown in the display.

Table 30 show ip bgp all dampening Field Descriptions

Field	Description
Half-life time	Time after which a penalty is decreased, in minutes. Once the interface has been assigned a penalty, the penalty is decreased by half after the half-life period. The process of reducing the penalty happens every 5 seconds. The range of the half-life is 1 to 45 minutes. The default is 1 minute.
Decay Time	Penalty value below which an unstable interface is unsuppressed, in seconds. The process of unsuppressing routers occurs at 10-second increments. The range of the reuse value is 1 to 20000 seconds. The default value is 750 seconds.
Max suppress penalty	Limit at which an interface is suppressed when its penalty exceeds that limit, in seconds. The default value is 2000 seconds.
Max suppress time	Maximum time that an interface can be suppressed, in minutes. This value effectively acts as a ceiling that the penalty value cannot exceed. The default value is four times the half-life period.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
show dampening interface	Displays a summary of the dampening parameters and status.

show ip bgp cidr-only

To display routes with classless interdomain routing (CIDR), use the **show ip bgp cidr-only** command in EXEC mode.

show ip bgp cidr-only

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ip bgp cidr-only** command in privileged EXEC mode:

```
Router# show ip bgp cidr-only

BGP table version is 220, local router ID is 172.16.73.131
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 192.168.0.0/8    172.16.72.24                         0 1878 ?
*> 172.16.0.0/16    172.16.72.30                         0 108 ?
```

Table 31 describes the significant fields shown in the display.

Table 31 show ip bgp cidr-only Field Descriptions

Field	Description
BGP table version is 220	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.

Table 31 show ip bgp cidr-only Field Descriptions (continued)

Field	Description
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a **network** router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

show ip bgp community

To display routes that belong to specified BGP communities, use the **show ip bgp community** command in EXEC mode.

show ip bgp community *community-number* [**exact**]

Syntax Description

community-number	Valid value is a community number in the range from 1 to 4294967200, or AA:NN (autonomous system-community number/2-byte number), **internet**, **no-export**, **local-as**, or **no-advertise**.
exact	(Optional) Displays only routes that have the same specified communities.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.0	The **local-as** community 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.

Examples

The following is sample output from the **show ip bgp community** command in privileged EXEC mode:

```
Router# show ip bgp community 111:12345 local-as

 BGP table version is 10, local router ID is 224.0.0.10
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop          Metric LocPrf Weight Path
 *> 172.16.2.2/32    10.43.222.2           0             0 222 ?
 *> 10.0.0.0         10.43.222.2           0             0 222 ?
 *> 10.43.0.0        10.43.222.2           0             0 222 ?
 *> 10.43.44.44/32   10.43.222.2           0             0 222 ?
 *  10.43.222.0/24   10.43.222.2           0             0 222 i
 *> 172.17.240.0/21  10.43.222.2           0             0 222 ?
 *> 192.168.212.0    10.43.222.2           0             0 222 i
 *> 172.31.1.0       10.43.222.2           0             0 222 ?
```

Table 32 describes the significant fields shown in the display.

Table 32 show ip bgp community Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show ip bgp community-list

To display routes that are permitted by the Border Gateway Protocol (BGP) community list, use the **show ip bgp community-list** command in user or privileged EXEC mode.

show ip bgp community-list {*community-list-number* | *community-list-name* [**exact-match**]}

Syntax Description

community-list-number	A standard or expanded community list number in the range from 1 to 500.
community-list-name	Community list name. The community list name can be standard or expanded.
exact-match	(Optional) Displays only routes that have an exact match.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.0(10)S	Named community list support was added.
12.0(16)ST	Named community lists support was integrated into Cisco IOS Release 12.0(16)ST.
12.1(9)E	Named community lists support was integrated into Cisco IOS Release 12.1(9)E.
12.2(8)T	Named community lists support was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB to support the Cisco 10000 Series Routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command requires you to specify an argument when used. The **exact-match** keyword is optional.

Examples

The following is sample output of the **show ip bgp community-list** command in privileged EXEC mode:

```
Router# show ip bgp community-list 20

BGP table version is 716977, local router ID is 192.168.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
   Network          Next Hop          Metric LocPrf Weight Path
* i10.3.0.0         10.0.22.1             0    100      0 1800 1239 ?
*>i                 10.0.16.1             0    100      0 1800 1239 ?
* i10.6.0.0         10.0.22.1             0    100      0 1800 690 568 ?
*>i                 10.0.16.1             0    100      0 1800 690 568 ?
* i10.7.0.0         10.0.22.1             0    100      0 1800 701 35 ?
*>i                 10.0.16.1             0    100      0 1800 701 35 ?
*                   10.92.72.24                         0 1878 704 701 35 ?
* i10.8.0.0         10.0.22.1             0    100      0 1800 690 560 ?
*>i                 10.0.16.1             0    100      0 1800 690 560 ?
*                   10.92.72.24                         0 1878 704 701 560 ?
* i10.13.0.0        10.0.22.1             0    100      0 1800 690 200 ?
*>i                 10.0.16.1             0    100      0 1800 690 200 ?
*                   10.92.72.24                         0 1878 704 701 200 ?
* i10.15.0.0        10.0.22.1             0    100      0 1800 174 ?
*>i                 10.0.16.1             0    100      0 1800 174 ?
* i10.16.0.0        10.0.22.1             0    100      0 1800 701 i
*>i                 10.0.16.1             0    100      0 1800 701 i
*                   10.92.72.24                         0 1878 704 701 i
```

Table 33 describes the significant fields shown in the display.

Table 33 show ip bgp community-list Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.

Table 33 show ip bgp community-list Field Descriptions (continued)

Field	Description
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show ip bgp dampened-paths

To display BGP dampened routes, use the **show ip bgp dampened-paths** command in EXEC mode.

show ip bgp dampened-paths

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

On the Cisco 10000 series router, use the **show ip bgp dampening dampened-paths** command to display BGP dampened routes.

Examples

The following is sample output from the **show ip bgp dampened-paths** command in privileged EXEC mode:

```
Router# show ip bgp dampened-paths

BGP table version is 10, local router ID is 172.29.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From             Reuse   Path
*d 10.0.0.0         172.16.232.177   00:18:4 100 ?
*d 10.2.0.0         172.16.232.177   00:28:5 100 ?
```

Table 34 describes the significant fields shown in the display.

Table 34 show ip bgp dampened-paths Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router	IP address of the router where route dampening is enabled.
*d	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.

Table 34 show ip bgp dampened-paths Field Descriptions (continued)

Field	Description
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear ip bgp dampening	Clears BGP route dampening information and unsuppresses the suppressed routes.

show ip bgp dampening dampened-paths

To display Border Gateway Protocol (BGP) dampened routes on the Cisco 10000 series router, use the **show ip bgp dampening dampened-paths** command in EXEC mode.

show ip bgp dampening dampened-paths [*community-list-number* | *community-list-name* [**exact-match**]]

Syntax Description

community-list-number	(Optional) Community list number. The range is from 1 to 500.
community-list-name	(Optional) Community list name.
exact-match	(Optional) Displays only routes that have an exact match.

Command Modes

EXEC

Command History

Release	Modification
12.2S	This command was introduced.

Usage Guidelines

For router platforms other than the Cisco 10000 series router, use the **show ip bgp dampened-paths** command to display BGP dampened routes.

Examples

The following example show how to display BGP dampened routes information:

```
Router# show ip bgp dampening dampened-paths

BGP table version is 10, local router ID is 172.29.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From             Reuse   Path
*d 10.0.0.0         172.16.232.177   00:18:4 100 ?
*d 10.2.0.0         172.16.232.177   00:28:5 100 ?
```

Table 35 describes the significant fields shown in the display.

Table 35 show ip bgp dampening dampened-paths Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.
*d	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.

Table 35 show ip bgp dampening dampened-paths Field Descriptions (continued)

Field	Description
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system (AS) path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear ip bgp dampening	Clears BGP route dampening information and unsuppresses the suppressed routes.
show dampening interface	Displays a summary of the dampening parameters and status.

show ip bgp dampening flap-statistics

To display Border Gateway Protocol (BGP) flap statistics for all paths on the Cisco 10000 series router, use the **show ip bgp dampening flap-statistics** command in privileged EXEC mode.

show ip bgp dampening flap-statistics [*ip-address* [**mask**] | **cidr-only** | **filter-list** **access-list-number** | **injected-paths** | **labels** | **prefix-list** *prefix-list* | **quote-regexp** *regexp* | **regexp** *regexp* | **route-map** *route-map-name* | **template** {**peer-policy** *template-name* | **peer-session** *template-name*}]

Syntax Description

ip-address	Specifies the IP address for the flap statistics you want to display.
mask	Specifies the mask to filter or match hosts that are part of the specified network.
cidr-only	Displays flap statistics for routes with classless interdomain routing (CIDR).
filter-list **access-list-number**	Displays flap statistics for routes that conform to the specified autonomous system (AS) path access list number.
injected-paths	Displays flap statistics for all injected paths.
labels	Displays flap statistics for IPv4 Network Layer Reachability Information (NLRI) labels.
prefix-list *prefix-list*	Filters output based on the specified prefix list.
quote-regexp *regexp*	Filters output based on the specified quoted expression.
regexp *regexp*	Filters output based on the specified regular expression.
route-map *route-map-name*	Filters output based on the specified route map.
template	Displays peer-policy or peer-session template information.
peer-policy *template-name*	Used with the **template** keyword, displays peer-policy template information for the specified template name.
peer-session *template-name*	Used with the **template** keyword, displays peer-session template information for the specified template name.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2S	This command was introduced.

Usage Guidelines

For router platforms other than the Cisco 10000 series router, use the **show ip bgp flap-statistics** command to display BGP flap statistics.

Examples

The following example show how to display the BGP flap statistics for routes with nonnatural network masks (CIDR):

```
Router# show ip bgp dampening flap-statistics cidr-only

BGP table version is 56, local router ID is 100.10.7.11
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
*>i205.0.5.0/30     100.10.5.11              0    100      0 i
*>i205.0.5.4/30     205.0.5.1                0    100      0 105 ?
*>i205.10.5.9/32    205.0.5.1                2    100      0 105 ?
*>i205.10.5.13/32   205.0.5.1                2    100      0 105 ?
*>i206.0.6.0/30     100.10.5.11              0    100      0 i
*>i206.0.6.4/30     206.0.6.1                0    100      0 106 ?
*>i206.10.6.9/32    206.0.6.1                2    100      0 106 ?
*>i206.10.6.13/32   206.0.6.1                2    100      0 106 ?
*> 207.0.7.0/30     0.0.0.0                  0         32768 i
*> 207.0.7.4/30     207.0.7.1                0             0 107 ?
*> 207.10.7.9/32    207.0.7.1                2             0 107 ?
*> 207.10.7.13/32   207.0.7.1                2             0 107 ?
*> 208.0.8.0/30     0.0.0.0                  0         32768 i
*> 208.0.8.4/30     208.0.8.1                0             0 108 ?
*> 208.10.8.9/32    208.0.8.1                2             0 108 ?
*> 208.10.8.13/32   208.0.8.1                2             0 108 ?
```

Table 35 describes the significant fields shown in the display.

Table 36 show ip bgp dampening flap-statistics cidr-only Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.
Status Codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the **set local-preference route-map** configuration command. The default value is 100.

Table 36 show ip bgp dampening flap-statistics cidr-only Field Descriptions (continued)

Field	Description
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear ip bgp flap-statistics	Clears BGP flap statistics.
show dampening interface	Displays a summary of the dampening parameters and status.

show ip bgp dampening parameters

To display detailed Border Gateway Protocol (BGP) dampening information on the Cisco 10000 series router, use the **show ip bgp dampening parameters** command in privileged EXEC mode.

show ip bgp dampening parameters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2S	This command was introduced.

Examples

The following example shows how to display detailed BGP dampening information:

```
Router# show ip bgp dampening parameters

dampening 15 750 2000 60 (DEFAULT)
  Half-life time      : 15 mins       Decay Time       : 2320 secs
  Max suppress penalty: 12000         Max suppress time: 60 mins
```

Table 37 describes the significant fields shown in the display.

Table 37 show ip bgp dampening parameters Field Descriptions

Field	Description
Half-life time	Time after which a penalty is decreased, in minutes. Once the interface has been assigned a penalty, the penalty is decreased by half after the half-life period. 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 1 minute.
Decay Time	Penalty value below which an unstable interface is unsuppressed, in seconds. The process of unsupressing routers occurs at 10 second increments. The range of the reuse value is 1 to 20000 seconds. The default value is 750 seconds.
Max suppress penalty	Limit at which an interface is suppressed when its penalty exceeds that limit, in seconds. The default value is 2000 seconds.
Max suppress time	Maximum time that an interface can be suppressed, in minutes. This value effectively acts as a ceiling that the penalty value cannot exceed. The default value is four times the half-life period.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear ip bgp dampening	Clears BGP dampening information.
show dampening interface	Displays a summary of the dampening parameters and status.

show ip bgp filter-list

To display routes that conform to a specified filter list, use the **show ip bgp filter-list** command in EXEC mode.

show ip bgp filter-list *access-list-number*

Syntax Description

access-list-number	Number of an autonomous system path access list. It can be a number from 1 to 199, or on the Cisco 10000 series router this is a number from 1 to 500.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ip bgp filter-list** command in privileged EXEC mode:

```
Router# show ip bgp filter-list 2

BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                         0 109 108 ?
*  172.16.1.0       172.16.72.30                         0 109 108 ?
*  172.16.11.0      172.16.72.30                         0 109 108 ?
*  172.16.14.0      172.16.72.30                         0 109 108 ?
*  172.16.15.0      172.16.72.30                         0 109 108 ?
*  172.16.16.0      172.16.72.30                         0 109 108 ?
*  172.16.17.0      172.16.72.30                         0 109 108 ?
*  172.16.18.0      172.16.72.30                         0 109 108 ?
*  172.16.19.0      172.16.72.30                         0 109 108 ?
*  172.16.24.0      172.16.72.30                         0 109 108 ?
*  172.16.29.0      172.16.72.30                         0 109 108 ?
*  172.16.30.0      172.16.72.30                         0 109 108 ?
*  172.16.33.0      172.16.72.30                         0 109 108 ?
*  172.16.35.0      172.16.72.30                         0 109 108 ?
*  172.16.36.0      172.16.72.30                         0 109 108 ?
*  172.16.37.0      172.16.72.30                         0 109 108 ?
*  172.16.38.0      172.16.72.30                         0 109 108 ?
*  172.16.39.0      172.16.72.30                         0 109 108 ?
```

Table 38 describes the significant fields shown in the display.

Table 38 show ip bgp filter-list Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP route to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a **network** router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

show ip bgp flap-statistics

To display BGP flap statistics, use the **show ip bgp flap-statistics** command in EXEC mode.

show ip bgp flap-statistics [**regexp** *regexp* | **filter-list** *access-list* | *ip-address mask* [**longer-prefix**]]

Syntax Description

regexp *regexp*	(Optional) Clears flap statistics for all the paths that match the regular expression.
filter-list *access-list*	(Optional) Clears flap statistics for all the paths that pass the access list.
ip-address	(Optional) Clears flap statistics for a single entry at this IP address.
mask	(Optional) Network mask applied to the value.
longer-prefix	(Optional) Displays flap statistics for more specific entries.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If no arguments or keywords are specified, the router displays flap statistics for all routes.

Examples

The following is sample output from the **show ip bgp flap-statistics** command in privileged EXEC mode:

```
Router# show ip bgp flap-statistics

BGP table version is 10, local router ID is 172.29.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From            Flaps Duration Reuse    Path
*d 10.0.0.0         172.29.232.177  4     00:13:31 00:18:10 100
*d 10.2.0.0         172.29.232.177  4     00:02:45 00:28:20 100
```

Table 39 describes the significant fields shown in the display.

Table 39 show ip bgp flap-statistics Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.
Network	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.
Flaps	Number of times the route has flapped.
Duration	Time (in hours:minutes:seconds) since the router noticed the first flap.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear ip bgp flap-statistics	Clears BGP flap statistics.

show ip bgp inconsistent-as

To display routes with inconsistent originating autonomous systems, use the **show ip bgp inconsistent-as** command in EXEC mode.

show ip bgp inconsistent-as

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ip bgp inconsistent-as** command in privileged EXEC mode:

```
Router# show ip bgp inconsistent-as

BGP table version is 87, local router ID is 172.19.82.53
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*  10.1.0.0         172.29.232.55          0             0 300 88 90 99 ?
*>                  172.29.232.52       2222             0 400 ?
*  172.29.0.0       172.29.232.55          0             0 300 90 99 88 200 ?
*>                  172.29.232.52       2222             0 400 ?
*  10.200.199.0     172.29.232.55          0             0 300 88 90 99 ?
*>                  172.29.232.52       2222             0 400 ?
```

show ip bgp injected-paths

To display all the injected paths in the Border Gateway Protocol (BGP) routing table, use the **show ip bgp injected-paths** command in user or privileged EXEC mode.

show ip bgp injected-paths

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

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(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Examples

The following is sample output from the **show ip bgp injected-paths** command in EXEC mode:

```
Router# show ip bgp injected-paths

BGP table version is 11, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.0.0       10.0.0.2                             0 ?
*> 172.17.0.0/16    10.0.0.2                             0 ?
```

Table 40 describes the significant fields shown in the display.

Table 40 show ip bgp injected-paths Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Table 40 show ip bgp injected-paths Field Descriptions (continued)

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show ip bgp ipv4

To display entries in the IP version 4 (IPv4) Border Gateway Protocol (BGP) routing table, use the **show ip bgp ipv4** command in privileged EXEC mode.

show ip bgp ipv4 {**mdt** {**all** | **rd** | **vrf**} | **multicast** | **tunnel** | **unicast**}

Syntax Description

mdt	Displays entries for multicast discovery tree sessions.
all	Displays all multicast discovery tree information.
rd	Displays information about the VPN route distinguisher in the MDT session.
vrf	Displays information about the VRF in the MDT session.
multicast	Displays entries for multicast sessions.
tunnel	Displays entries for tunnel sessions.
unicast	Displays entries for unicast sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(29)S	The **mdt** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	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	The **mdt** keyword was added.

Examples

The following is sample output from the **show ip bgp ipv4 unicast** command:

```
Router# show ip bgp ipv4 unicast

 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1              0            0  300 i
*> 10.10.20.0/24   172.16.10.1              0            0  300 i
*  10.20.10.0/24   172.16.10.1              0            0  300 i
```

The following is sample output from the **show ip bgp ipv4 multicast** command:

```
Router# show ip bgp ipv4 multicast

 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1              0             0  300 i
*> 10.10.20.0/24   172.16.10.1              0             0  300 i
*  10.20.10.0/24   172.16.10.1              0             0  300 i
```

Table 41 describes the significant fields shown in the display.

Table 41 show ip bgp ipv4 unicast Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is damped. • h—The table entry history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is displayed at the end of each line in the table. It can be one of the following values: • i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from an Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Related Commands

Command	Description
clear ip bgp ipv4 mdt	Resets multicast discovery tree IPv4 BGP address-family sessions.
show ip bgp	Displays entries in the BGP routing table.

show ip bgp ipv4 multicast

To display IP Version 4 multicast database-related information, use the **show ip bgp ipv4 multicast** command in EXEC mode.

show ip bgp ipv4 multicast [*command*]

Syntax Description

command	(Optional) Any multiprotocol BGP command supported by the **show ip bgp ipv4 multicast** *command*.

Command Modes

EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command in conjunction with the **show ip rpf** command to determine if IP multicast routing is using multiprotocol BGP routes.

To determine which multiprotocol BGP commands are supported by the **show ip bgp ipv4 multicast** command, enter the following command while in EXEC mode:

```
Router# show ip bgp ipv4 multicast ?
```

The **show ip bgp ipv4 multicast** command replaces the **show ip mbgp** command.

Examples

The following is sample output from the **show ip bgp ipv4 multicast** command:

```
Router# show ip bgp ipv4 multicast

MBGP table version is 6, local router ID is 192.168.200.66
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*> 10.0.20.16/28     0.0.0.0                0      0 32768 i
*> 10.0.35.16/28     0.0.0.0                0      0 32768 i
*> 10.0.36.0/28      0.0.0.0                0      0 32768 i
*> 10.0.48.16/28     0.0.0.0                0      0 32768 i
*> 10.2.0.0/16       0.0.0.0                0      0 32768 i
*> 10.2.1.0/24       0.0.0.0                0      0 32768 i
*> 10.2.2.0/24       0.0.0.0                0      0 32768 i
*> 10.2.3.0/24       0.0.0.0                0      0 32768 i
*> 10.2.7.0/24       0.0.0.0                0      0 32768 i
*> 10.2.8.0/24       0.0.0.0                0      0 32768 i
```

```
*> 10.2.10.0/24      0.0.0.0                0      0 32768 i
*> 10.2.11.0/24      0.0.0.0                0      0 32768 i
*> 10.2.12.0/24      0.0.0.0                0      0 32768 i
*> 10.2.13.0/24      0.0.0.0                0      0 32768 i
```

Table 42 describes the significant fields shown in the display.

Table 42 show ip bgp ipv4 multicast Field Descriptions

Field	Description
MBGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is historical. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration or address family configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Related Commands

Command	Description
show ip rpf	Displays how IP multicast routing does RPF.

show ip bgp ipv4 multicast summary

To display a summary of IP Version 4 multicast database-related information, use the **show ip bgp ipv4 multicast summary** command in EXEC mode.

show ip bgp ipv4 multicast summary

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
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 **show ip bgp ipv4 multicast summary** command replaces the **show ip mbgp summary** command.

Examples

The following is sample output from the **show ip bgp ipv4 multicast summary** command:

```
Router# show ip bgp ipv4 multicast summary

BGP router identifier 10.0.33.34, local AS number 34
BGP table version is 5, main routing table version 1
4 network entries and 6 paths using 604 bytes of memory
5 BGP path attribute entries using 260 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
2 BGP community entries using 48 bytes of memory
2 BGP route-map cache entries using 32 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP activity 8/28 prefixes, 12/0 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.33.35      4    35     624     624        5    0    0 10:13:46        3
```

Table 43 describes the significant fields shown in the display.

Table 43 show ip bgp ipv4 multicast summary Field Descriptions

Field	Description
Neighbor	IP address of configured neighbor in the multicast routing table.
V	Version of multiprotocol BGP used.
AS	Autonomous system to which the neighbor belongs.

Table 43 show ip bgp ipv4 multicast summary Field Descriptions (continued)

Field	Description
MsgRcvd	Number of messages received from the neighbor.
MsgSent	Number of messages sent to the neighbor.
TblVer	Number of the table version, which is incremented each time the table changes.
InQ	Number of messages received in the input queue.
OutQ	Number of messages ready to go in the output queue.
Up/Down	Days and hours that the neighbor has been up or down (no information in the State column means the connection is up).
State/PfxRcd	State of the neighbor/number of routes received. If no state is indicated, the state is up.

Related Commands

Command	Description
show ip rpf	Displays how IP multicast routing does RPF.

show ip bgp l2vpn

To display Layer 2 Virtual Private Network (L2VPN) address family information from the Border Gateway Protocol (BGP) table, use the **show ip bgp l2vpn** command in user EXEC or privileged EXEC mode.

With BGP show Command Argument

show ip bgp l2vp vpls {**all** | **rd** *route-distinguisher*} [*bgp-keyword*]

With IP Prefix and Mask Length Syntax

show ip bgp l2vp vpls {**all** | **rd** *route-distinguisher*} [*ip-prefix/length* [**bestpath**] [**longer-prefixes** [**injected**]] [**multipaths**] [**shorter-prefixes** [*mask-length*]] [**subnets**]]

With Network Address Syntax

show ip bgp l2vp vpls {**all** | **rd** *route-distinguisher*} [*network-address* [*mask* | **bestpath** | **multipaths**] [**bestpath**] [**longer-prefixes** [**injected**]] [**multipaths**] [**shorter-prefixes** [*mask-length*]] [**subnets**]]

Syntax Description

vpls	Displays L2VPN address family database information for the Virtual Private LAN Service (VPLS) subsequent address family identifier (SAFI).
all	Displays the complete L2VPN database.
rd *route-distinguisher*	Displays prefixes that match the specified route distinguisher.
bgp-keyword	(Optional) Argument representing a **show ip bgp** command keyword that can be added to this command. See Table 44.
ip-prefix/length	(Optional) The IP prefix address (in dotted decimal format) and the length of the mask (0 to 32). The slash mark must be included.
bestpath	(Optional) Displays the best path for the specified prefix.
longer-prefixes	(Optional) Displays the route and more specific routes.
injected	(Optional) Displays more specific routes that were injected because of the specified prefix.
multipaths	(Optional) Displays the multipaths for the specified prefix.
shorter-prefixes	(Optional) Displays the less specific routes.
mask-length	(Optional) The length of the mask as a number in the range from 0 to 32. Prefixes longer than the specified mask length are displayed.
subnets	(Optional) Displays the subnet routes for the specified prefix.
network-address	(Optional) The IP address of a network in the BGP routing table.
mask	(Optional) The mask of the network address, in dotted decimal format.

Command Default

If no arguments or keywords are specified, this command displays the complete L2VPN database.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Table 44 displays optional **show ip bgp** command keywords that can be configured with the **show ip bgp l2vpn** command. Replace the *bgp-keyword* argument with the appropriate keyword from the table. For more details about each command in its **show ip bgp** *bgp-keyword* form, see the *Cisco IOS IP Routing Protocols Command Reference*, Release 12.2SR.

Table 44 Optional show ip bgp Command Keywords and Descriptions

Keyword	Description
community	Displays routes that match a specified community
community-list	Displays routes that match a specified community list.
dampening	Displays paths suppressed because of dampening (BGP route from peer is up and down).
extcommunity-list	Displays routes that match a specified extcommunity list.
filter-list	Displays routes that conform to the filter list.
inconsistent-as	Displays only routes that have inconsistent autonomous systems of origin.
neighbors	Displays details about TCP and BGP neighbor connections.
oer-paths	Displays all OER-managed path information.
paths [*regexp*]	Displays autonomous system path information. If the optional *regexp* argument is entered, the autonomous system paths that are displayed match the autonomous system path regular expression.
peer-group	Displays information about peer groups.
pending-prefixes	Displays prefixes that are pending deletion.
prefix-list	Displays routes that match a specified prefix list.
quote-regexp	Displays routes that match the quoted autonomous system path regular expression.
regexp	Displays routes that match the autonomous system path regular expression.
replication	Displays the replication status update groups.
route-map	Displays routes that match the specified route map.
rt-filter-list	Displays the specified inbound route target filter list.
summary	Displays a summary of BGP neighbor status.
update-group	Displays information on update groups.

Examples

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **all** keywords are used to display the complete L2VPN database:

```
Router# show ip bgp l2vpn vpls all

BGP table version is 5, local router ID is 192.168.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 45000:100
*> 45000:100:172.17.1.1/96
                    0.0.0.0                            32768 ?
*>i45000:100:172.18.2.2/96
                    172.16.1.2               0    100      0 ?
Route Distinguisher: 45000:200
*> 45000:200:172.17.1.1/96
                    0.0.0.0                            32768 ?
*>i45000:200:172.18.2.2/96
                    172.16.1.2               0    100      0 ?
```

Table 45 describes the significant fields shown in the display.

Table 45 show ip bgp l2vpn vpls all Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is a historical entry. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session. • r—The table entry failed to install in the routing information base (RIB) table. • S—The table entry is Stale (old). This entry is useful in BGP graceful restart situations.

Table 45 show ip bgp l2vpn vpls all Field Descriptions (continued)

Field	Description
Origin codes	Origin of the entry. The origin code is displayed at the end of each line in the table. It can be one of the following values: • i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. • e—Entry originated from an Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.
Route Distinguisher	Route distinguisher that identifies a set of routing and forwarding tables used in virtual private networks.

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **rd** keywords are used to display the L2VPN information that matches the route distinguisher 45000:100. Note that the information displayed is a subset of the information displayed using the **all** keyword.

```
Router# show ip bgp l2vpn vpls rd 45000:100

BGP table version is 5, local router ID is 192.168.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 45000:100
*> 45000:100:172.17.1.1/96
                    0.0.0.0                              32768 ?
*>i45000:100:172.18.2.2/96
                    172.16.1.2               0    100      0 ?
```

Related Commands

Command	Description
address-family l2vpn	Enters address family configuration mode to configure a routing session using L2VPN endpoint provisioning information.

show ip bgp neighbors

To display information about Border Gateway Protocol (BGP) and TCP connections to neighbors, use the **show ip bgp neighbors** command in user or privileged EXEC mode.

show ip bgp [**ipv4** {**multicast** | **unicast**} | **vpnv4 all | vpnv6 unicast all**] **neighbors** [**slow** | *ip-address* | *ipv6-address* [**advertised-routes** | **dampened-routes** | **flap-statistics** | **paths** [*reg-exp*] | **policy** [**detail**] | **received prefix-filter** | **received-routes** | **routes**]]

Syntax Description

ipv4 {**multicast** | **unicast**}	(Optional) Displays peers in the IPv4 address family.
vpnv4 all	(Optional) Displays peers in the VPNv4 address family.
vpnv6 unicast all	(Optional) Displays peers in the VPNv6 address family.
slow	(Optional) Displays information about dynamically configured slow peers.
ip-address	(Optional) Displays information about the IPv4 neighbor. If this argument is omitted, information about all neighbors is displayed.
ipv6-address	(Optional) Displays information about the IPv6 neighbor.
advertised-routes	(Optional) Displays all routes that have been advertised to neighbors.
dampened-routes	(Optional) Displays the dampened routes received from the specified neighbor.
flap-statistics	(Optional) Displays the flap statistics of the routes learned from the specified neighbor (for external BGP peers only).
paths *reg-exp*	(Optional) Displays autonomous system paths learned from the specified neighbor. An optional regular expression can be used to filter the output.
policy	(Optional) Displays the policies applied to this neighbor per address family.
detail	(Optional) Displays detailed policy information such as route maps, prefix lists, community lists, access control lists (ACLs), and autonomous system path filter lists.
received prefix-filter	(Optional) Displays the prefix-list (outbound route filter [ORF]) sent from the specified neighbor.
received-routes	(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	(Optional) Displays all routes that are received and accepted. The output displayed when this keyword is entered is a subset of the output displayed by the **received-routes** keyword.

Command Default

The output of this command displays information for all neighbors.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

OS Release	Modification
12.0(18)S	The output was modified to display the no-prepend configuration option, and this command was integrated into Cisco IOS Release 12.0(18)S.
12.0(21)ST	The output was modified to display Multiprotocol Label Switching (MPLS) label information.
12.0(22)S	Support for the BGP graceful restart capability was integrated into the output. Support for the Cisco 12000 series routers (Engine 0 and Engine 2) was also added.
12.0(25)S	The **policy** and **detail** keywords were added.
12.0(27)S	The command output was modified to support the BGP TTL Security Check feature and to display explicit-null label information.
12.0(31)S	Support for the Bidirectional Forwarding Detection (BFD) feature was integrated into the output.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
S Release	**Modification**
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.2(18)SXE	Support for the Bidirectional Forwarding Detection (BFD) feature was integrated into the output.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA, and the output was modified to support BGP TCP path MTU discovery.
12.2(33)SRB	Support for the **policy** and **detail** keywords was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	The output was modified to support BGP dynamic neighbors.
12.2(33)SRC	The output was modified to support BGP graceful restart per peer.
12.2(33)SB	The output was modified to support the BFD and the BGP graceful restart per peer features, and support for the **policy** and **detail** keywords was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI1	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)SRE	This command was modified. The command output was modified to support the BGP best external and BGP additional path features. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was modified. The **slow** keyword was added.
15.1(1)S	This command was modified to display the Layer 2 VPN address family if graceful restart (GR) or nonstop forwarding (NSF) is enabled.

Mainline and T Release	Modification
10.0	This command was introduced.
11.2	The **received-routes** keyword was added.
12.2(4)T	The **received** and **prefix-filter** keywords were added, and this command was integrated into Cisco IOS Release 12.2(4)T.
12.2(15)T	Support for the BGP graceful restart capability was integrated into the output.
12.3(7)T	The command output was modified to support the BGP TTL Security Check feature and to display explicit-null label information.
12.4(4)T	Support for the Bidirectional Forwarding Detection (BFD) feature was integrated into the output.
12.4(11)T	Support for the **policy** and **detail** keywords was integrated into Cisco IOS Release 12.4(11)T.
12.4(20)T	The output was modified to support BGP TCP path MTU discovery.
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE	**Modification**
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
Cisco IOS XE Release 3.1S	This command was modified. The **slow** keyword was added.

Usage Guidelines

Use the **show ip bgp neighbors** command to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

Prefix activity is displayed based on the number of prefixes that are advertised and withdrawn. Policy denials display the number of routes that were advertised but then ignored based on the function or attribute that is displayed in the output.

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.

Cisco IOS Releases 12.0(25)S, 12.4(11)T, 12.2(33)SRB, 12.2(33)SB, and Later Releases

When BGP neighbors use multiple levels of peer templates, it can be difficult to determine which policies are applied to the neighbor.

In Cisco IOS Releases 12.0(25)S, 12.4(11)T, 12.2(33)SRB, 12.2(33)SB, and later releases, the **policy** and **detail** keywords were added to display the inherited policies and the policies configured directly on the specified neighbor. Inherited policies are policies that the neighbor inherits from a peer-group or a peer-policy template.

Examples

Example output is different for the various keywords available for the **show ip bgp neighbors** command. Examples using the various keywords appear in the following sections:

- show ip bgp neighbors: Example, page 487
- show ip bgp neighbors (4-Byte Autonomous System Numbers): Example, page 493
- show ip bgp neighbors advertised-routes: Example, page 493
- show ip bgp neighbors paths: Example, page 495
- show ip bgp neighbors received prefix-filter: Example, page 495
- show ip bgp neighbors policy: Example, page 495
- Cisco IOS Release 12.0(31)S, 12.4(4)T, 12.2(18)SXE, and 12.2(33)SB: Example, page 496
- Cisco IOS Release 12.2(33)SRA and 12.4(20)T: Example, page 496
- Cisco IOS Release 12.2(33)SXH: Example, page 496
- Cisco IOS Releases 12.2(33)SRC and 12.2(33)SB: Example, page 497
- Cisco IOS Release 15.1(1)S: Example, page 497

show ip bgp neighbors: Example

The following example shows output for the BGP neighbor at 10.108.50.2. This neighbor is an internal BGP (iBGP) peer. This neighbor supports the route refresh and graceful restart capabilities.

```
Router# show ip bgp neighbors 10.108.50.2

BGP neighbor is 10.108.50.2,  remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is
   60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    MPLS Label capability: advertised and received
    Graceful Restart Capability: advertised
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        115
  Default minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
  BGP additional-paths computation is enabled
  BGP advertise-best-external is enabled
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
```

```
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              0          0
    Prefixes Total:                0          0
    Implicit Withdraw:             0          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          0
    Used as multipath:           n/a          0

                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Total:                               0          0
  Number of NLRIs in the update sent: max 0, min 0

  Connections established 3; dropped 2
  Last reset 00:24:26, due to Peer closed the session
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x68B944):
Timer          Starts    Wakeups            Next
Retrans            27          0             0x0
TimeWait            0          0             0x0
AckHold            27         18             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 3915509457  snduna: 3915510016  sndnxt: 3915510016     sndwnd:  15826
irs:  233567076  rcvnxt:  233567616  rcvwnd:      15845  delrcvwnd:    539

SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08
```

Table 46 describes the significant fields shown in the display. Fields that are preceded by the asterisk character (*) are displayed only when the counter has a nonzero value.

Table 46 show ip bgp neighbors Field Descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number.
remote AS	Autonomous system number of the neighbor.

Table 46 show ip bgp neighbors Field Descriptions (continued)

Field	Description
local AS 300 no-prepend (not shown in display)	Verifies that the local autonomous system number is not prepended to received external routes. This output supports the hiding of the local autonomous systems when migrating autonomous systems.
internal link	"internal link" is displayed for iBGP neighbors. "external link" is displayed for external BGP (eBGP) neighbors.
BGP version	BGP version being used to communicate with the remote router.
remote router ID	IP address of the neighbor.
BGP state	Finite state machine (FSM) stage of session negotiation.
up for	Time, in hhmmss, that the underlying TCP connection has been in existence.
Last read	Time, in hhmmss, since BGP last received a message from this neighbor.
last write	Time, in hhmmss, since BGP last sent a message to this neighbor.
hold time	Time, in seconds, that BGP will maintain the session with this neighbor without receiving a messages.
keepalive interval	Time interval, in seconds, at which keepalive messages are transmitted to this neighbor.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor. "advertised and received" is displayed when a capability is successfully exchanged between two routers.
Route Refresh	Status of the route refresh capability.
MPLS Label Capability	Indicates that MPLS labels are both sent and received by the eBGP peer.
Graceful Restart Capability	Status of the graceful restart capability.
Address family IPv4 Unicast	IP Version 4 unicast-specific properties of this neighbor.
Message statistics	Statistics organized by message type.
InQ depth is	Number of messages in the input queue.
OutQ depth is	Number of messages in the output queue.
Sent	Total number of transmitted messages.
Received	Total number of received messages.
Opens	Number of open messages sent and received.
notifications	Number of notification (error) messages sent and received.
Updates	Number of update messages sent and received.
Keepalives	Number of keepalive messages sent and received.
Route Refresh	Number of route refresh request messages sent and received.
Total	Total number of messages sent and received.
Default minimum time between...	Time, in seconds, between advertisement transmissions.

Table 46 show ip bgp neighbors Field Descriptions (continued)

Field	Description
For address family:	Address family to which the following fields refer.
BGP table version	Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.
neighbor version	Number used by the software to track prefixes that have been sent and those that need to be sent.
...update-group	Number of update-group member for this address family.
Prefix activity	Prefix statistics for this address family.
Prefixes current	Number of prefixes accepted for this address family.
Prefixes total	Total number of received prefixes.
Implicit Withdraw	Number of times that a prefix has been withdrawn and readvertised.
Explicit Withdraw	Number of times that prefix has been withdrawn because it is no longer feasible.
Used as bestpath	Number of received prefixes installed as bestpaths.
Used as multipath	Number of received prefixes installed as multipaths.
* Saved (soft-reconfig)	Number of soft resets performed with a neighbor that supports soft reconfiguration. This field is displayed only if the counter has a nonzero value.
* History paths	This field is displayed only if the counter has a nonzero value.
* Invalid paths	Number of invalid paths. This field is displayed only if the counter has a nonzero value.
Local Policy Denied Prefixes	Prefixes denied due to local policy configuration. Counters are updated for inbound and outbound policy denials. The fields under this heading are displayed only if the counter has a nonzero value.
* route-map	Displays inbound and outbound route-map policy denials.
* filter-list	Displays inbound and outbound filter-list policy denials.
* prefix-list	Displays inbound and outbound prefix-list policy denials.
* Ext Community	Displays only outbound extended community policy denials.
* AS_PATH too long	Displays outbound AS-path length policy denials.
* AS_PATH loop	Displays outbound AS-path loop policy denials.
* AS_PATH confed info	Displays outbound confederation policy denials.
* AS_PATH contains AS 0	Displays outbound denials of autonomous system (AS) 0.
* NEXT_HOP Martian	Displays outbound martian denials.
* NEXT_HOP non-local	Displays outbound non-local next-hop denials.
* NEXT_HOP is us	Displays outbound next-hop-self denials.
* CLUSTER_LIST loop	Displays outbound cluster-list loop denials.
* ORIGINATOR loop	Displays outbound denials of local originated routes.

Table 46 show ip bgp neighbors Field Descriptions (continued)

Field	Description
* unsuppress-map	Displays inbound denials due to an unsuppress-map.
* advertise-map	Displays inbound denials due to an advertise-map.
* VPN Imported prefix	Displays inbound denials of VPN prefixes.
* Well-known Community	Displays inbound denials of well-known communities.
* SOO loop	Displays inbound denials due to site-of-origin.
* Bestpath from this peer	Displays inbound denials because the bestpath came from the local router.
* Suppressed due to dampening	Displays inbound denials because the neighbor or link is in a dampening state.
* Bestpath from iBGP peer	Deploys inbound denials because the bestpath came from an iBGP neighbor.
* Incorrect RIB for CE	Deploys inbound denials due to RIB errors for a CE router.
* BGP distribute-list	Displays inbound denials due to a distribute list.
Number of NLRIs...	Number of network layer reachability attributes in updates.
Connections established	Number of times a TCP and BGP connection has been successfully established.
dropped	Number of times that a valid session has failed or been taken down.
Last reset	Time since this peering session was last reset. The reason for the reset is displayed on this line.
External BGP neighbor may be... (not shown in the display)	Indicates that the BGP TTL security check is enabled. The maximum number of hops that can separate the local and remote peer is displayed on this line.
Connection state	Connection status of the BGP peer.
Connection is ECN Disabled	Explicit congestion notification status (enabled or disabled).
Local host: 10.108.50.1, Local port: 179	IP address of the local BGP speaker. BGP port number 179.
Foreign host: 10.108.50.2, Foreign port: 42698	Neighbor address and BGP destination port number.
Enqueued packets for retransmit:	Packets queued for retransmission by TCP.
Event Timers	TCP event timers. Counters are provided for starts and wakeups (expired timers).
Retrans	Number of times a packet has been retransmitted.
TimeWait	Time waiting for the retransmission timers to expire.
AckHold	Acknowledgment hold timer.
SendWnd	Transmission (send) window.
KeepAlive	Number of keepalive packets.
GiveUp	Number times a packet is dropped due to no acknowledgment.
PmtuAger	Path MTU discovery timer.

Table 46 show ip bgp neighbors Field Descriptions (continued)

Field	Description
DeadWait	Expiration timer for dead segments.
iss:	Initial packet transmission sequence number.
snduna:	Last transmission sequence number that has not been acknowledged.
sndnxt:	Next packet sequence number to be transmitted.
sndwnd:	TCP window size of the remote neighbor.
irs:	Initial packet receive sequence number.
rcvnxt:	Last receive sequence number that has been locally acknowledged.
rcvwnd:	TCP window size of the local host.
delrcvwnd:	Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT:	A calculated smoothed round-trip timeout.
RTTO:	Round-trip timeout.
RTV:	Variance of the round-trip time.
KRTT:	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.
minRTT:	Smallest recorded round-trip timeout (hard-wire value used for calculation).
maxRTT:	Largest recorded round-trip timeout.
ACK hold:	Length of time the local host will delay an acknowledgment to carry (piggyback) additional data.
IP Precedence value:	IP precedence of the BGP packets.
Datagrams	Number of update packets received from a neighbor.
Rcvd:	Number of received packets.
with data	Number of update packets sent with data.
total data bytes	Total amount of data received, in bytes.
Sent	Number of update packets sent.
Second Congestion	Number of update packets with data sent.
Datagrams: Rcvd	Number of update packets received from a neighbor.
out of order:	Number of packets received out of sequence.
with data	Number of update packets received with data.
Last reset	Elapsed time since this peering session was last reset.
unread input bytes	Number of bytes of packets still to be processed.
retransmit	Number of packets retransmitted.

Table 46 show ip bgp neighbors Field Descriptions (continued)

Field	Description
fastretransmit	Number of duplicate acknowledgments retransmitted for an out of order segment before the retransmission timer expires.
partialack	Number of retransmissions for partial acknowledgements (transmissions before or without subsequent acknowledgments).
Second Congestion	Number of second retransmissions sent due to congestion.

show ip bgp neighbors (4-Byte Autonomous System Numbers): Example

The following partial example shows output for several external BGP neighbors in autonomous systems with 4-byte autonomous system numbers, 65536 and 65550. 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# show ip bgp neighbors

BGP neighbor is 192.168.1.2,  remote AS 65536, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 02:03:38, last write 02:03:38, hold time is 120, keepalive interval is 70
seconds
  Configured hold time is 120, keepalive interval is 70 seconds
  Minimum holdtime from neighbor is 0 seconds
.
.
.
BGP neighbor is 192.168.3.2,  remote AS 65550, external link
 Description: finance
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 02:03:48, last write 02:03:48, hold time is 120, keepalive interval is 70
seconds
  Configured hold time is 120, keepalive interval is 70 seconds
  Minimum holdtime from neighbor is 0 seconds
```

show ip bgp neighbors advertised-routes: Example

The following example displays routes advertised for only the 172.16.232.178 neighbor:

```
Router# show ip bgp neighbors 172.16.232.178 advertised-routes

BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop          Metric LocPrf Weight Path
*>i10.0.0.0      172.16.232.179         0    100      0 ?
*> 10.20.2.0     10.0.0.0               0         32768 i
```

Table 47 describes the significant fields shown in the display.

Table 47 show ip bgp neighbors advertised-routes Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.
local router ID	IP address of the local BGP speaker.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened and will not be advertised to BGP neighbors. • h—The table entry does not contain the best path based on historical information. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system used to forward a packet to the destination network. An entry of 0.0.0.0 indicates that there are non-BGP routes in the path to the destination network.
Metric	If shown, this is the value of the interautonomous system metric. This field is not used frequently.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show ip bgp neighbors paths: Example

The following is example output from the **show ip bgp neighbors** command entered with the **paths** keyword:

```
Router# show ip bgp neighbors 172.29.232.178 paths ^10

Address    Refcount Metric Path
0x60E577B0        2     40 10 ?
```

Table 48 describes the significant fields shown in the display.

Table 48 show ip bgp neighbors paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Refcount	Number of routes using that path.
Metric	Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	Autonomous system path for that route, followed by the origin code for that route.

show ip bgp neighbors received prefix-filter: Example

The following example shows that a prefix-list that filters all routes in the 10.0.0.0 network has been received from the 192.168.20.72 neighbor:

```
Router# show ip bgp neighbors 192.168.20.72 received prefix-filter

Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
   seq 5 deny 10.0.0.0/8 le 32
```

Table 49 describes the significant fields shown in the display.

Table 49 show ip bgp neighbors received prefix-filter Field Descriptions

Field	Description
Address family	Address family mode in which the prefix filter is received.
ip prefix-list	Prefix list sent from the specified neighbor.

show ip bgp neighbors policy: Example

The following sample output shows the policies applied to the neighbor at 192.168.1.2. The output displays both inherited policies and policies configured on the neighbor device. Inherited polices are policies that the neighbor inherits from a peer-group or a peer-policy template.

```
Router# show ip bgp neighbors 192.168.1.2 policy

Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
 route-map ROUTE in
Inherited polices:
 prefix-list NO-MARKETING in
 route-map ROUTE in
 weight 300
 maximum-prefix 10000
```

Cisco IOS Release 12.0(31)S, 12.4(4)T, 12.2(18)SXE, and 12.2(33)SB: Example

The following is sample output from the **show ip bgp neighbors** command that verifies that Bidirectional Forwarding Detection (BFD) is being used to detect fast fallover for the BGP neighbor that is a BFD peer:

```
Router# show ip bgp neighbors

BGP neighbor is 172.16.10.2,  remote AS 45000, external link
.
.
.
 Using BFD to detect fast fallover
```

Cisco IOS Release 12.2(33)SRA and 12.4(20)T: Example

The following is sample output from the **show ip bgp neighbors** command that verifies that BGP TCP path maximum transmission unit (MTU) discovery is enabled for the BGP neighbor at 172.16.1.2:

```
Router# show ip bgp neighbors 172.16.1.2

BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

Cisco IOS Release 12.2(33)SXH: Example

The following is sample output from the **show ip bgp neighbors** command that verifies that the neighbor 192.168.3.2 is a member of the peer group, group192, and belongs to the subnet range group 192.168.0.0/16, which shows that this BGP neighbor was dynamically created:

```
Router# show ip bgp neighbors 192.168.3.2

BGP neighbor is *192.168.3.2,  remote AS 50000, external link
 Member of peer-group group192 for session parameters
 Belongs to the subnet range group: 192.168.0.0/16
  BGP version 4, remote router ID 192.168.3.2
  BGP state = Established, up for 00:06:35
  Last read 00:00:33, last write 00:00:25, hold time is 180, keepalive intervals
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
```

```
    Opens:                  1          1
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             7          7
    Route Refresh:          0          0
    Total:                  8          8
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1/0
  Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
  group192 peer-group member
.
.
.
```

Cisco IOS Releases 12.2(33)SRC and 12.2(33)SB: Example

The following is partial output from the **show ip bgp neighbors** command that verifies the status of the BGP graceful restart capability for the external BGP peer at 192.168.3.2. Graceful restart is shown as disabled for this BGP peer.

```
Router# show ip bgp neighbors 192.168.3.2

BGP neighbor is 192.168.3.2,  remote AS 50000, external link
 Inherits from template S2 for session parameters
  BGP version 4, remote router ID 192.168.3.2
  BGP state = Established, up for 00:01:41
  Last read 00:00:45, last write 00:00:45, hold time is 180, keepalive intervals
  Neighbor sessions:
    1 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
.
.
.
Address tracking is enabled, the RIB does have a route to 192.168.3.2
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
```

Cisco IOS Release 15.1(1)S: Example

The following is partial output from the **show ip bgp neighbors** command. For this release, the display includes the Layer 2 VFN address family information if graceful restart or NSF is enabled.

For more information about the other fields shown in the display, see Table 46 on page 488.

```
Router# show ip bgp neighbors

Load for five secs: 2%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:49:17.034 GMT Wed Sep 22 2010

BGP neighbor is 10.1.1.3,  remote AS 2, internal link
  BGP version 4, remote router ID 10.1.1.3
  BGP state = Established, up for 00:14:32
  Last read 00:00:30, last write 00:00:43, hold time is 180, keepalive interval is 60
seconds
```

```
 Neighbor sessions:
   1 active, is not multisession capable (disabled)
 Neighbor capabilities:
   Route refresh: advertised and received(new)
   Four-octets ASN Capability: advertised and received
   Address family IPv4 Unicast: advertised and received
   Address family L2VPN Vpls: advertised and received
   Graceful Restart Capability: advertised and received
     Remote Restart timer is 120 seconds
     Address families advertised by peer:
       IPv4 Unicast (was not preserved), L2VPN Vpls (was not preserved)
   Multisession Capability:
 Message statistics:
   InQ depth is 0
   OutQ depth is 0

                        Sent       Rcvd
   Opens:                  1          1
   Notifications:          0          0
   Updates:                4         16
   Keepalives:            16         16
   Route Refresh:          0          0
   Total:                 21         33
 Default minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast
 Session: 10.1.1.3
 BGP table version 34, neighbor version 34/0
 Output queue size : 0
 Index 1, Advertise bit 0
 1 update-group member
 Slow-peer detection is disabled
 Slow-peer split-update-group dynamic is disabled
                              Sent       Rcvd
 Prefix activity:             ----       ----
   Prefixes Current:             2         11 (Consumes 572 bytes)
   Prefixes Total:               4         19
   Implicit Withdraw:            2          6
   Explicit Withdraw:            0          2
   Used as bestpath:           n/a          7
   Used as multipath:          n/a          0

                                Outbound    Inbound
 Local Policy Denied Prefixes:  --------    -------
   NEXT_HOP is us:                   n/a          1
   Bestpath from this peer:           20        n/a
   Bestpath from iBGP peer:            8        n/a
   Invalid Path:                      10        n/a
   Total:                             38          1
 Number of NLRIs in the update sent: max 2, min 0
 Last detected as dynamic slow peer: never
 Dynamic slow peer recovered: never

For address family: L2VPN Vpls
 Session: 10.1.1.3
 BGP table version 8, neighbor version 8/0
 Output queue size : 0
 Index 1, Advertise bit 0
 1 update-group member
 Slow-peer detection is disabled
 Slow-peer split-update-group dynamic is disabled
                              Sent       Rcvd
 Prefix activity:             ----       ----
   Prefixes Current:             1          1 (Consumes 68 bytes)
```

```
    Prefixes Total:                 2          1
    Implicit Withdraw:              1          0
    Explicit Withdraw:              0          0
    Used as bestpath:             n/a          1
    Used as multipath:            n/a          0

                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Bestpath from this peer:              4        n/a
    Bestpath from iBGP peer:              1        n/a
    Invalid Path:                         2        n/a
    Total:                                7          0
  Number of NLRIs in the update sent: max 1, min 0
  Last detected as dynamic slow peer: never
  Dynamic slow peer recovered: never

  Address tracking is enabled, the RIB does have a route to 10.1.1.3
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is enabled, restart-time 120 seconds, stalepath-time 360 seconds
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Mininum incoming TTL 0, Outgoing TTL 255
Local host: 10.1.1.1, Local port: 179
Foreign host: 10.1.1.3, Foreign port: 48485
Connection tableid (VRF): 0

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0xE750C):
Timer          Starts    Wakeups            Next
Retrans            18          0             0x0
TimeWait            0          0             0x0
AckHold            22         20             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
Linger              0          0             0x0
iss: 3196633674  snduna: 3196634254  sndnxt: 3196634254     sndwnd:  15805
irs: 1633793063  rcvnxt: 1633794411  rcvwnd:      15037  delrcvwnd:   1347

SRTT: 273 ms, RTTO: 490 ms, RTV: 217 ms, KRTT: 0 ms
minRTT: 2 ms, maxRTT: 300 ms, ACK hold: 200 ms
Status Flags: passive open, gen tcbs
Option Flags: nagle, path mtu capable

Datagrams (max data segment is 1436 bytes):
Rcvd: 42 (out of order: 0), with data: 24, total data bytes: 1347
Sent: 40 (retransmit: 0 fastretransmit: 0),with data: 19, total data bytes: 579
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
neighbor send-label	Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.
neighbor send-label explicit-null	Enables a BGP router to send MPLS labels with explicit-null information for a CSC-CE router and BGP routes to a neighboring CSC-PE router.
router bgp	Configures the BGP routing process.

show ip bgp paths

To display all the BGP paths in the database, use the **show ip bgp paths** command in EXEC mode.

show ip bgp paths

Cisco 10000 Series Router

show ip bgp paths *regexp*

Syntax Description

regexp	Regular expression to match the BGP autonomous system paths.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
12.2(33)SRE	This command was modified. Support for displaying 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.

Examples

The following is sample output from the **show ip bgp paths** command in privileged EXEC mode:

```
Router# show ip bgp paths

Address    Hash Refcount Metric Path
0x60E5742C    0        1      0 i
0x60E3D7AC    2        1      0 ?
0x60E5C6C0   11        3      0 10 ?
0x60E577B0   35        2     40 10 ?
```

Table 50 describes the significant fields shown in the display.

Table 50 show ip bgp paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Hash	Hash bucket where path is stored.
Refcount	Number of routes using that path.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The autonomous system path for that route, followed by the origin code for that route.

show ip bgp peer-group

To display information about BGP peer groups, use the **show ip bgp peer-group** command in user EXEC or privileged EXEC mode.

show ip bgp peer-group [*peer-group-name*] [**summary**]

Syntax Description

peer-group-name	(Optional) Displays information about a specific peer group.
summary	(Optional) Displays a summary of the status of all the members of a peer group.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
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, and the output was modified to support BGP dynamic neighbors.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S, with the modified output to support BGP dynamic neighbors.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S, with the modified output to support BGP dynamic neighbors.

Examples

The following is sample output from the **show ip bgp peer-group** command for a peer group named internal in privileged EXEC mode:

```
Router# show ip bgp peer-group internal

BGP peer-group is internal, remote AS 100
  BGP version 4
  Minimum time between advertisement runs is 5 seconds

 For address family:IPv4 Unicast
  BGP neighbor is internal, peer-group internal, members:
           10.1.1.1         10.1.1.2
  Index 3, Offset 0, Mask 0x8
  Incoming update AS path filter list is 53
  Outgoing update AS path filter list is 54
  Route map for incoming advertisements is MAP193
  Route map for outgoing advertisements is MAP194
  Update messages formatted 0, replicated 0
```

The following output from the **show ip bgp peer-group** command shows information about a configured listen range group, group192. In Cisco IOS Release 12.2(33)SXH, 15.0(1)S, and XE Release 3.1S and later releases, the BGP dynamic neighbor feature introduced the ability to support the dynamic creation of BGP neighbor peers using a subnet range associated with a peer group (listen range group).

```
Router# show ip bgp peer-group group192

BGP peer-group is group192,  remote AS 40000
  BGP peergroup group192 listen range group members:
  192.168.0.0/16
  BGP version 4
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP neighbor is group192, peer-group external, members:
  *192.168.3.2
  Index 0, Offset 0, Mask 0x0
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 0
```

show ip bgp quote-regexp

To display routes matching the autonomous system path regular expression, use the **show ip bgp quote-regexp** command in privileged EXEC mode.

show ip bgp quote-regexp *regexp*

Syntax Description

regexp	The regular expression to match the Border Gateway Protocol (BGP) autonomous system paths. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command. **Note** The regular expression has to be an exact match.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
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 displaying 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.

Release	Modification
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
12.2(33)SRE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

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.

Examples

The following is sample output from the **show ip bgp quote-regexp** command in EXEC mode:

```
Router# show ip bgp quote-regexp "^10_" | begin 10.40

*> 10.40.0.0/20     10.10.10.10                          0 10 2548 1239 10643 i
*> 10.40.16.0/20    10.10.10.10                          0 10 2548 6172 i
*> 10.40.32.0/19    10.10.10.10                          0 10 2548 6172 i
*> 10.41.0.0/19     10.10.10.10                          0 10 2548 3356 3703 ?
*> 10.42.0.0/17     10.10.10.10                          0 10 2548 6172 i
```

Note Although the columns in the above display are not labeled, see Table 51 for detailed information.

Table 51 describes the significant fields shown in the display from left to right.

Table 51 show ip bgp quote-regexp Field Descriptions

Field	Description
Status codes	Status of the table entry; for example, * in the above display. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session. r—The table entry failed to install in the routing table. S—The table entry is a stale route.
Network	IP address of a network entity; for example, 24.40.0.0/20 in the above display.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network; for example, 10.10.10.10. in the above display. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.; for example, 0 in the above display.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command; for example, 10 in the above display. The default value is 100.
Weight	Weight of the route as set via autonomous system filters; for example, 2548 in the above display.
Path	Autonomous system paths to the destination network; for example, 1239 in the above display. There can be one entry in this field for each autonomous system in the path.
Origin codes	Origin of the entry; for example, ? in the above display. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.

The following output from the **show ip bgp quote-regexp** command shows routes that match the quoted regular expression for the 4-byte autonomous system number 65550. The 4-byte autonomous system number is displayed in the default asplain format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Router# show ip bgp quote-regexp "^65550$"

BGP table version is 4, 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
*> 10.2.2.0/24      192.168.3.2              0             0 65550 i
```

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.
router bgp	Configures the BGP routing process.
show ip bgp regexp	Displays routes matching the autonomous system path regular expression.

show ip bgp regexp

To display routes matching the autonomous system path regular expression, use the **show ip bgp regexp** command in EXEC mode.

show ip bgp regexp *regexp*

Syntax Description

regexp	Regular expression to match the BGP autonomous system paths. • 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 Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
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 displaying 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.

Release	Modification
12.2(33)SRE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

To ensure a smooth transition we recommend that all BGP speakers within an autonomous system that is identified using a 4-byte autonomous system number, are upgraded to support 4-byte autonomous system numbers.

Examples

The following is sample output from the **show ip bgp regexp** command in privileged EXEC mode:

```
Router# show ip bgp regexp 108$

BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                         0 109 108 ?
*  172.16.1.0       172.16.72.30                         0 109 108 ?
*  172.16.11.0      172.16.72.30                         0 109 108 ?
*  172.16.14.0      172.16.72.30                         0 109 108 ?
*  172.16.15.0      172.16.72.30                         0 109 108 ?
*  172.16.16.0      172.16.72.30                         0 109 108 ?
*  172.16.17.0      172.16.72.30                         0 109 108 ?
*  172.16.18.0      172.16.72.30                         0 109 108 ?
*  172.16.19.0      172.16.72.30                         0 109 108 ?
*  172.16.24.0      172.16.72.30                         0 109 108 ?
*  172.16.29.0      172.16.72.30                         0 109 108 ?
*  172.16.30.0      172.16.72.30                         0 109 108 ?
*  172.16.33.0      172.16.72.30                         0 109 108 ?
*  172.16.35.0      172.16.72.30                         0 109 108 ?
*  172.16.36.0      172.16.72.30                         0 109 108 ?
*  172.16.37.0      172.16.72.30                         0 109 108 ?
*  172.16.38.0      172.16.72.30                         0 109 108 ?
*  172.16.39.0      172.16.72.30                         0 109 108 ?
```

The following 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. 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 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
```

The following is sample output from the **show ip bgp regexp** command after the **bgp asnotation dot** command has been entered to display 4-byte autonomous system numbers in dot notation 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, or later release. The dot notation is the only format for 4-byte autonomous system numbers in Cisco IOS Release 12.0(32)S12, 12.4(24)T, or Cisco IOS XE Release 2.3.

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 ^1\.14$

BGP table version is 4, 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 1.14   i
```

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.
router bgp	Configures the BGP routing process.
show ip bgp quote-regexp	Displays routes matching the autonomous system path regular expression.

show ip bgp replication

To display update replication statistics for Border Gateway Protocol (BGP) update groups, use the **show ip bgp replication** command in EXEC mode.

show ip bgp replication [**index-group** | **ip-address**]

Syntax Description

index-group	(Optional) Displays update replication statistics for the update group with corresponding index number will be displayed. The range of update-group index numbers is from 1 to 4294967295.
ip-address	(Optional) Displays the IP address of a single neighbor for which update-group statistics will be displayed.

Command Modes

EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(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 output of this command displays BGP update-group replication statistics.

When a change to outbound policy occurs, the router automatically recalculates update-group memberships and applies the changes by triggering an outbound soft reset after a 3-minute timer expires. This behavior is designed to provide the network operator with time to change the configuration if a mistake is made. You can manually enable an outbound soft reset before the timer expires by entering the **clear ip bgp** *ip-address* **soft out** command.

Examples

The following sample output from the **show ip bgp replication** command shows update-group replication information for all neighbors:

```
Router# show ip bgp replication

BGP Total Messages Formatted/Enqueued : 0/0

     Index     Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
         1 internal        1       10.4.9.21        0        0      0      0
         2 internal        2        10.4.9.5        0        0      0      0
```

The following sample output from the **show ip bgp replication** command shows update-group statistics for the 10.4.9.5 neighbor:

```
Router# show ip bgp replication 10.4.9.5

     Index     Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
         2 internal        2        10.4.9.5        0        0      0      0
```

Table 52 describes the significant fields shown in the display.

Table 52 show ip bgp replication Field Descriptions

Field	Description
Index	Index number of the update group.
Type	Type of peer (internal or external).
Members	Number of members in the dynamic update peer group.
Leader	First member of the dynamic update peer group.

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection or session.
clear ip bgp update-group	Clears BGP update-group member sessions.
debug ip bgp groups	Displays information related to the processing of BGP update groups.
show ip bgp peer-group	Displays information about BGP update groups.

show ip bgp rib-failure

To display Border Gateway Protocol (BGP) routes that failed to install in the Routing Information Base (RIB) table, use the **show ip bgp rib-failure** command in privileged EXEC mode.

show ip bgp rib-failure

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3	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(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ip bgp rib-failure** command:

```
Router# show ip bgp rib-failure

Network          Next Hop                    RIB-failure   RIB-NH Matches
10.1.15.0/24     10.1.35.5          Higher admin distance             n/a
10.1.16.0/24     10.1.15.1          Higher admin distance             n/a
```

Table 53 describes the significant fields shown in the display.

Table 53 show ip bgp rib-failure Field Descriptions

Field	Description
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.

Table 53 show ip bgp rib-failure Field Descriptions (continued)

Field	Description
RIB-failure	Cause of RIB failure. Higher admin distance means that a route with a better (lower) administrative distance such as a static route already exists in the IP routing table.
RIB-NH Matches	Route status that applies only when Higher admin distance appears in the RIB-failure column and **bgp suppress-inactive** is configured for the address family being used. There are three choices: • Yes—Means that the route in the RIB has the same next hop as the BGP route or next hop recurses down to the same adjacency as the BGP nexthop. • No—Means that the next hop in the RIB recurses down differently from the next hop of the BGP route. • n/a—Means that **bgp suppress-inactive** is not configured for the address family being used.

Related Commands

Command	Description
bgp suppress-inactive	Configures a router to suppress the advertisement of BGP routes that are not installed in the RIB and FIB tables.
clear ip bgp	Resets a BGP connection or session.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

show ip bgp rtfilter

To display information about BGP route target (RT) filtering, use the **show ip bgp rtfilter** command in user EXEC or privileged EXEC mode.

show ip bgp rtfilter unicast {**all** | **default** | **rt** {*ASN*:*nn* | *ip-address*:*nn*}}

Syntax Description

unicast	Display unicast information.
all	Display RT information for all VPNs.
default	Display the default RT filter.
rt	Display a specific RT filter prefix.
ASN:*nn*	Autonomous system number, followed by a colon and number.
ip-address:*nn*	IP address, followed by a colon and a number.

Command Modes

User EXEC (>)
Privileged EXEC (#)

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.

Usage Guidelines

Use this command if you have configured the BGP: RT Constrained Route Distribution feature and you want to display RT filter information.

Note If you enter the **all** keyword, there are many more optional keywords available that are not shown here.

Examples

The following is sample output from the **show ip bgp rtfilter unicast all** command:

```
Router# show ip bgp rtfilter unicast all

BGP table version is 14, local router ID is 192.168.7.7
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, f
RT-Filter
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network Next HopMetricLocPrf Weight Path
*>i0:0:0:0192.168.2.201000 i
*>i1:2:1:100192.168.6.601000 i
* i1:2:3:3192.168.2.201000 i
*>  0.0.0.0    32768 i
*>i1:2:150:1192.168.6.601000 i
* i1:2:200:200192.168.2.201000 i
*>  0.0.0.0    32768 i
Router#
```

Table 27 describes the fields shown in the display.

Table 54 show ip bgp rtfilter Field Descriptions

Field	Description
Network	RT filter prefix.
Next Hop	Next hop in the RT filter prefix.
Metric	BGP metric associated with the RT filter prefix.
LocPref	BGP local preference.
Weight	BGP weight.
Path	Path information associated with the RT prefix.

The following is sample output from the **show ip bgp rtfilter all summary** command:

```
Router# show ip bgp rtfilter all summary

BGP router identifier 192.168.7.7, local AS number 1
BGP table version is 14, main routing table version 14
5 network entries using 820 bytes of memory
7 path entries using 336 bytes of memory
2/2 BGP path/bestpath attribute entries using 256 bytes of memory
1 BGP rrinfo entries using 24 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1484 total bytes of memory
BGP activity 7/0 prefixes, 14/5 paths, scan interval 60 secs

NeighborVAS MsgRcvd MsgSent TblVer InQ OutQ Up/Down  State/PfxRcd
192.168.2.241 1 312140   0   0   00:03:21        5
Router#
```

Related Commands

Command	Description
address-family rtfilter unicast	Enters address family configuration mode and enables Automated Route Target Filtering with a BGP peer.
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.
show ip bgp rtfilter all summary	Displays summary information about RT filtering.

show ip bgp summary

To display the status of all Border Gateway Protocol (BGP) connections, use the **show ip bgp summary** command in user EXEC or privileged EXEC mode.

show ip bgp [**ipv4** {**multicast** | **unicast**} | **vpnv4 all | vpnv6 unicast all** | **topology{*|** *routing-topology-instance-name*}] [**update-group**] **summary** [**slow**]

Syntax Description

ipv4 {**multicast** | **unicast**}	(Optional) Displays peers in the IPv4 address family.
vpnv4 all	(Optional) Displays peers in the VPNv4 address family.
vpnv6 unicast all	(Optional) Displays peers in the VPNv6 address family.
topology	(Optional) Displays routing topology information.
*****	(Optional) Displays allrouting topology instances.
routing-topology-instance-name	(Optional) Displays routing topology information for that instance.
update-group	(Optional) Includes information about the update group of the peers.
slow	(Optional) Displays only information about dynamically configured slow peers.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0	Support for the **neighbor maximum-prefix** command was added to the output.
12.2	• The number of networks and paths displayed in the output was split out to two separate lines. • A field was added to display multipath entries in the routing table.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	A line was added to the output to display the advertised bitfield cache entries and associated memory usage.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH, and the output was modified to support BGP dynamic neighbors.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for displaying 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 displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
12.2(33)SRE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was modified. The **slow** keyword was added.
Cisco IOS XE Release 3.1S	This command was modified. The **slow** keyword was added.

Usage Guidelines

The **show ip bgp summary** command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors.

A prefix is an IP address and network mask. It can represent an entire network, a subset of a network, or a single host route. A path is a route to a given destination. By default, BGP will install only a single path for each destination. If multipath routes are configured, BGP will install a path entry for each multipath route, and only one multipath route will be marked as the bestpath.

BGP attribute and cache entries are displayed individually and in combinations that affect the bestpath selection process. The fields for this output are displayed when the related BGP feature is configured or attribute is received. Memory usage is displayed in bytes.

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.

Examples

The following is sample output from the **show ip bgp summary** command in privileged EXEC mode:

```
Router# show ip bgp summary

BGP router identifier 172.16.1.1, local AS number 100
BGP table version is 199, main routing table version 199
37 network entries using 2850 bytes of memory
59 path entries using 5713 bytes of memory
18 BGP path attribute entries using 936 bytes of memory
```

```
2 multipath network entries and 4 multipath paths
10 BGP AS-PATH entries using 240 bytes of memory
7 BGP community entries using 168 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
90 BGP advertise-bit cache entries using 1784 bytes of memory
36 received paths for inbound soft reconfiguration
BGP using 34249 total bytes of memory
Dampening enabled. 4 history paths, 0 dampened paths
BGP activity 37/2849 prefixes, 60/1 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
10.100.1.1      4   200      26      22      199    0    0 00:14:23 23
10.200.1.1      4   300      21      51      199    0    0 00:13:40 0
```

Table 55 describes the significant fields shown in the display. Fields that are preceded by the asterisk character (*) are not shown in the above output.

Table 55 show ip bgp summary Field Descriptions

Field	Description
BGP router identifier	In order of precedence and availability, the router identifier specified by the **bgp router-id** command, a loopback address, or the highest IP address.
BGP table version	Internal version number of BGP database.
main routing table version	Last version of BGP database that was injected into the main routing table.
...network entries	Number of unique prefix entries in the BGP database.
...using ... bytes of memory	Amount of memory, in bytes, that is consumed for the path, prefix, or attribute entry displayed on the same line.
...path entries using	Number of path entries in the BGP database. Only a single path entry will be installed for a given destination. If multipath routes are configured, a path entry will be installed for each multipath route.
...multipath network entries using	Number of multipath entries installed for a given destination.
* ...BGP path/bestpath attribute entries using	Number of unique BGP attribute combinations for which a path is selected as the bestpath.
* ...BGP rrinfo entries using	Number of unique ORIGINATOR and CLUSTER_LIST attribute combinations.
...BGP AS-PATH entries using	Number of unique AS_PATH entries.
...BGP community entries using	Number of unique BGP community attribute combinations.
*...BGP extended community entries using	Number of unique extended community attribute combinations.
BGP route-map cache entries using	Number of BGP route-map match and set clause combinations. A value of 0 indicates that the route cache is empty.
...BGP filter-list cache entries using	Number of filter-list entries that match an AS-path access list permit or deny statements. A value of 0 indicates that the filter-list cache is empty.

Table 55 show ip bgp summary Field Descriptions (continued)

Field	Description
BGP advertise-bit cache entries using	(Cisco IOS Release 12.4(11)T and later releases only) Number of advertised bitfield entries and the associated memory usage. A bitfield entry represents a piece of information (one bit) that is generated when a prefix is advertised to a peer. The advertised bit cache is built dynamically when required.
...received paths for inbound soft reconfiguration	Number paths received and stored for inbound soft reconfiguration.
BGP using...	Total amount of memory, in bytes, used by the BGP process.
Dampening enabled...	Indicates that BGP dampening is enabled. The number of paths that carry an accumulated penalty and the number of dampened paths are displayed on this line.
BGP activity...	Displays the number of times that memory has been allocated or released for a path or prefix.
Neighbor	IP address of the neighbor.
V	BGP version number spoken to the neighbor.
AS	Autonomous system number.
MsgRcvd	Number of messages received from the neighbor.
MsgSent	Number of messages sent to the neighbor.
TblVer	Last version of the BGP database that was sent to the neighbor.
InQ	Number of messages queued to be processed from the neighbor.
OutQ	Number of messages queued to be sent to the neighbor.
Up/Down	The length of time that the BGP session has been in the Established state, or the current status if not in the Established state.
State/PfxRcd	Current state of the BGP session, and the number of prefixes that have been received from a neighbor or peer group. When the maximum number (as set by the **neighbor maximum-prefix** command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is set to Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the **neighbor shutdown** command.

The following output from the **show ip bgp summary** command shows that the BGP neighbor 192.168.3.2 was dynamically created and is a member of the listen range group, group192. The output also shows that the IP prefix range of 192.168.0.0/16 is defined for the listen range group named group192. In Cisco IOS Release 12.2(33)SXH and later releases, the BGP dynamic neighbor feature introduced the ability to support the dynamic creation of BGP neighbor peers using a subnet range associated with a peer group (listen range group).

```
Router# show ip bgp summary

BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1
```

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1

BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

The following output from the **show ip bgp summary** command shows two BGP neighbors, 192.168.1.2 and 192.168.3.2, in different 4-byte autonomous system numbers, 65536 and 65550. The local autonomous system 65538 is also a 4-byte autonomous system number and the numbers are displayed in the default asplain format. 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# 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 output from the **show ip bgp summary** command shows the same two BGP neighbors, but the 4-byte autonomous system numbers are displayed in asdot notation format. To change the display format the **bgp asnotation dot** command must be configured in router configuration mode. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, or Cisco IOS XE Release 2.3 or later releases.

```
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
```

The following example displays sample output of the **show ip bgp summary slow** command:

```
Router> show ip bgp summary slow
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 37, main routing table version 37
36 network entries using 4608 bytes of memory
36 path entries using 1872 bytes of memory
1/1 BGP path/bestpath attribute entries using 124 bytes of memory
1 BGP rrinfo entries using 24 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 6700 total bytes of memory
BGP activity 46/0 prefixes, 48/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
6.6.6.6 4 100 11 10 1 0 0 00:44:20 0
```

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 router-id	Configures a fixed router ID for the local BGP routing process.
neighbor maximum-prefix	Controls how many prefixes can be received from a BGP neighbor.
neighbor shutdown	Disables a BGP neighbor or peer group.
neighbor slow-peer split-update-group dynamic	Causes a dynamically detected slow peer to be moved to a slow update group.
router bgp	Configures the BGP routing process.

show ip bgp template peer-policy

To display locally configured peer policy templates, use the **show ip bgp template peer-policy** command in user EXEC or privileged EXEC mode.

show ip bgp template peer-policy [*policy-template-name* [**detail**]]

Syntax Description

policy-template-name	(Optional) Name of a locally configured peer policy template.
detail	(Optional) Displays detailed policy information such as route maps, prefix lists, community lists, access control lists (ACLs), and AS-path filter lists.

Command Default

If a peer policy template is not specified using the *policy-template-name* argument, all peer policy templates will be displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.0(25)S	The **detail** keyword was added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.4(11)T	Support for the **detail** keyword was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command and support for the **detail** keyword were integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	Support for the **detail** keyword was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command is used to display locally configured peer policy templates. The output can be filtered to display a single peer policy template using the *policy-template-name* argument. This command also supports all standard output modifiers.

When BGP neighbors use multiple levels of peer templates it can be difficult to determine which policies are associated with a specific template. In Cisco IOS Release 12.0(25)S, 12.4(11)T, 12.2(33)SRB, 12.2(33)SB, and later releases, the **detail** keyword was added to display the detailed configuration of local and inherited policies associated with a specific template. Inherited policies are policies that the template inherits from other peer-policy templates.

Examples

The **show ip bgp template peer-policy** command is used to verify the configuration of local peer policy templates. The following sample output shows the peer policy templates named GLOBAL and NETWORK1. The output also shows that the GLOBAL template was inherited by the NETWORK1 template.

```
Router# show ip bgp template peer-policy

Template:GLOBAL, index:1.
Local policies:0x80840, Inherited polices:0x0
 *Inherited by Template NETWORK1, index:2
Locally configured policies:
  prefix-list NO-MARKETING in
  weight 300
  maximum-prefix 10000
Inherited policies:

Template:NETWORK1, index:2.
Local policies:0x1, Inherited polices:0x80840
This template inherits:
  GLOBAL, index:1, seq_no:10, flags:0x1
Locally configured policies:
  route-map ROUTE in
Inherited policies:
  prefix-list NO-MARKETING in
  weight 300
  maximum-prefix 10000
```

Table 56 describes the significant fields shown in the display.

Table 56 show ip bgp template peer-policy Field Descriptions

Field	Description
Template	Name of the peer template.
index	The sequence number in which the displayed template is processed.
Local policies	Displays the hexadecimal value of locally configured policies.
Inherited polices	Displays the hexadecimal value of inherited policies. The 0x0 value is displayed when no templates are inherited.
Locally configured policies	Displays a list of commands that are locally configured in a peer policy template.
Inherited policies	Displays a list of commands that are inherited from a peer template.

The following sample output of the **show ip bgp template peer-policy** command with the **detail** keyword displays details of the template named NETWORK1, which includes the inherited template named GLOBAL. The output in this example displays the configuration commands of the locally configured route map and prefix list and the inherited prefix list.

```
Router# show ip bgp template peer-policy NETWORK1 detail

Template:NETWORK1, index:2.
Local policies:0x1, Inherited polices:0x80840
This template inherits:
  GLOBAL, index:1, seq_no:10, flags:0x1
Locally configured policies:
  route-map ROUTE in
```

```
Inherited policies:
  prefix-list NO-MARKETING in
  weight 300
  maximum-prefix 10000

Template:NETWORK1 <detail>
Locally configured policies:
  route-map ROUTE in
route-map ROUTE, permit, sequence 10
  Match clauses:
    ip address prefix-lists: DEFAULT
ip prefix-list DEFAULT: 1 entries
   seq 5 permit 10.1.1.0/24

  Set clauses:
  Policy routing matches: 0 packets, 0 bytes

Inherited policies:
  prefix-list NO-MARKETING in
ip prefix-list NO-MARKETING: 1 entries
   seq 5 deny 10.2.2.0/24
```

Related Commands

Command	Description
inherit peer-policy	Configures a peer policy template to inherit the configuration from another peer policy template.
template peer-policy	Creates a peer policy template and enters policy-template configuration mode.

show ip bgp template peer-session

To display peer policy template configurations, use the **show ip bgp template peer-session** command in user EXEC and privileged EXEC mode.

show ip bgp template peer-session [*session-template-name*]

Syntax Description

session-template-name	(Optional) Name of a locally configured peer session template.

Defaults

If a peer session template is not specified with the *session-template-name* argument, all peer session templates will be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used to display locally configured peer session templates. The output can be filtered to display a single peer session template with the *peer-session-name* argument. This command also supports all standard output modifiers.

Examples

The **show ip bgp template peer-session** command is used to verify the configuration of local peer session templates. The following example shows the peer session templates named INTERNAL-BGP and CORE1. The output also shows that INTERNAL-BGP is inherited by CORE1.

```
Router# show ip bgp template peer-session

Template:INTERNAL-BGP, index:1
Local policies:0x21, Inherited polices:0x0
 *Inherited by Template CORE1, index= 2
Locally configured session commands:
 remote-as 202
 timers 30 300
Inherited session commands:
```

```
Template:CORE1, index:2
Local policies:0x180, Inherited polices:0x21
This template inherits:
  INTERNAL-BGP index:1 flags:0x0
Locally configured session commands:
 update-source loopback 1
 description CORE-123
Inherited session commands:
 remote-as 202
 timers 30 300
```

Table 57 describes the significant fields shown in the display.

Table 57 show ip bgp template peer-session Field Descriptions

Field	Description
Template:	Name of the peer template.
index:	The sequence number in which the displayed template is processed.
Local policies:	Displays the hexadecimal value of locally configured policies.
Inherited polices:	Displays the hexadecimal value of inherited policies. The 0x0 value is displayed when no templates are inherited.
Locally configured session commands:	Displays a list of commands that are locally configured in a peer template.
Inherited session commands:	Displays a list of commands that are inherited from a peer session template.

Related Commands

Command	Description
inherit peer-session	Configures a peer session template to inherit the configuration from another peer session template.
template peer-session	Creates a peer session template and enters session-template configuration mode.

show ip bgp update-group

To display information about the Border Gateway Protocol (BGP) update groups, use the **show ip bgp update-group** command in user EXEC or privileged EXEC mode.

show ip bgp update-group [*index-group* | *ip-address* | *ipv6-address*] [**summary**]

Syntax Description

index-group	(Optional) Update group type with its corresponding index number. The range of update-group index numbers is from 1 to 4294967295.
ip-address	(Optional) IP address of a single neighbor who is a member of an update group.
ipv6-address	(Optional) IPv6 address of a single neighbor who is member of an update group.
summary	(Optional) Displays a summary of update-group member information. The output can be filtered to show information for a single index group or peer with the *index-group*, *ip-address*, or *ipv6-address* argument.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S. The *ipv6-address* argument was added.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display information about BGP update groups. When a change to BGP outbound policy occurs, the router automatically recalculates update group memberships and applies the changes by triggering an outbound soft reset after a 1-minute timer expires. This behavior is designed to provide the network operator with time to change the configuration if a mistake is made. You can manually enable an outbound soft reset before the timer expires by entering the **clear ip bgp** *ip-address* **soft out** command.

Note In Cisco IOS Release 12.0(25)S, 12.3(2)T, and prior releases, the update group recalculation delay timer is set to 3 minutes.

Examples

The following sample output from the **show ip bgp update-group** command shows update group information for all neighbors:

```
Router# show ip bgp update-group

BGP version 4 update-group 1, internal, Address Family: IPv4 Unicast
  BGP Update version : 0, messages 0/0
  Route map for outgoing advertisements is COST1
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 0
  Minimum time between advertisement runs is 5 seconds
  Has 1 member:
  10.4.9.21

BGP version 4 update-group 2, internal, Address Family: IPv4 Unicast
  BGP Update version : 0, messages 0/0
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 0
  Minimum time between advertisement runs is 5 seconds
  Has 2 members:
  10.4.9.5 10.4.9.8
```

Table 58 describes the significant fields shown in the display.

Table 58 show ip bgp update-group Field Descriptions

Field	Description
BGP version	BGP version.
update-group	Update-group number and type (internal or external).
Update messages formatted..., replicated...	Number of update messages that have been formatted and replicated.
Number of NLRIs...	NLRI information sent in update.
Minimum time between...	Minimum time, in seconds, between update advertisements.
Has...	Number of member listed by IP address in the update group.

The following sample output from the **show ip bgp update-group** command shows a summary of update-group information for the 10.4.9.8 neighbor:

```
Router# show ip bgp update-group 10.4.9.8 summary

Summary for Update-group 2 :
-----------------------------
BGP router identifier 10.4.9.4, local AS number 101
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.4.9.5        4   101      35      35        1    0    0 00:26:22        0
10.4.9.8        4   101      39      39        1    0    0 00:26:21        0
```

Table 59 describes the significant fields shown in the display.

Table 59 show ip bgp update-group summary Field Descriptions

Field	Description
Summary for Update-group...	Update-group number.
BGP router identifier...	IP address and AS number for specified peer.

Table 59 show ip bgp update-group summary Field Descriptions (continued)

Field	Description
update messages formatted..., replicated...	Number of update messages that have been formatted and replicated.
BGP table version...	Displays incremental changes in the BGP routing table.
Neighbor...	Specific peer information and statistics, including IP address and AS number.

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection or session.
clear ip bgp update-group	Clears BGP update-group member sessions.
debug ip bgp groups	Displays information related to the processing of BGP update groups.
show ip bgp replication	Displays BGP update-group replication statistics.

show ip bgp vpnv4 all sso summary

To display information about Border Gateway Protocol (BGP) peers that support BGP nonstop routing (NSR) with stateful switchover (SSO), use the **show ip bgp vpn4 sso summary** command in privileged EXEC mode.

show ip bgp vpnv4 all sso summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **show ip bgp vpnv4 all sso summary** command is used to display the number of BGP neighbors that are in SSO mode.

Examples

The following is sample output from the **show ip bgp vpnv4 all sso summary** command:

```
Router# show ip bgp vpnv4 all sso summary

   Stateful switchover support enabled for 40 neighbors
```

Table 60 describes the significant fields shown in the display.

Table 60 show ip bgp vpnv4 all sso summary Field Descriptions

Field	Description
Stateful Switchover support enabled for	Indicates the number of BGP neighbors that are in SSO mode.

Related Commands

Command	Description
neighbor ha-mode sso	Configures a BGP neighbor to support SSO.

show ip bgp vpnv4

To display Virtual Private Network Version 4 (VPNv4) address information from the Border Gateway Protocol (BGP) table, use the **show ip bgp vpnv4** command in user EXEC or privileged EXEC mode.

show ip bgp vpnv4 {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} [*ip-prefix*/*length* [**longer-prefixes**]] [*network-address* [*mask*] [**longer-prefixes**]] [**cidr-only**] [**community**] [**community-list**] [**dampening**] [**filter-list**] [**flap-statistics**] [**inconsistent-as**] [**labels**] [**neighbors**] [**paths** [*line*]] [**peer-group**] [**quote-regexp**] [**regexp**] [**rib-failure**] [**summary**]

Syntax Description

all	Displays the complete VPNv4 database.
rd *route-distinguisher*	Displays Network Layer Reachability Information (NLRI) prefixes that match the named route distinguisher.
vrf *vrf-name*	Displays NLRI prefixes associated with the named VPN routing and forwarding (VRF) instance.
ip-prefix/length	(Optional) IP prefix address (in dotted decimal format) and the length of the mask (0 to 32). The slash mark must be included.
longer-prefixes	(Optional) Displays the entry, if any, that exactly matches the specified prefix parameter and all entries that match the prefix in a "longest-match" sense. That is, prefixes for which the specified prefix is an initial substring.
network-address	(Optional) IP address of a network in the BGP routing table.
mask	(Optional) Mask of the network address, in dotted decimal format.
cidr-only	(Optional) Displays only routes that have nonclassful net masks.
community	(Optional) Displays routes that match this community.
community-list	(Optional) Displays routes that match this community list.
dampening	(Optional) Displays paths suppressed because of dampening (BGP route from peer is up and down).
filter-list	(Optional) Displays routes that conform to the filter list.
flap-statistics	(Optional) Displays flap statistics of routes.
inconsistent-as	(Optional) Displays only routes that have inconsistent autonomous systems of origin.
labels	(Optional) Displays incoming and outgoing BGP labels for each NLRI prefix.
neighbors	(Optional) Displays details about TCP and BGP neighbor connections.
paths	(Optional) Displays path information.
line	(Optional) A regular expression to match the BGP autonomous system paths.
peer-group	(Optional) Displays information about peer groups.
quote-regexp	(Optional) Displays routes that match the autonomous system path regular expression.
regexp	(Optional) Displays routes that match the autonomous system path regular expression.

rib-failure	(Optional) Displays BGP routes that failed to install in the VRF table.
summary	(Optional) Displays BGP neighbor status.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(2)T	The output of the **show ip bgp vpnv4 all** *ip-prefix* command was enhanced to display attributes including multipaths and a best path to the specified network.
12.0(21)ST	The **tags** keyword was replaced by the **labels** keyword to conform to the MPLS guidelines. This command was integrated into Cisco IOS Release 12.0(21)ST.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.0(27)S	The output of the **show ip bgp vpnv4 all labels** command was enhanced to display explicit-null label information.
12.3	The **rib-failure** keyword was added for VRFs.
12.2(22)S	The output of the **show ip bgp vpnv4 vrf** *vrf-name* **labels** command was modified so that directly connected VRF networks no longer display as aggregate; no label appears instead.
12.2(25)S	This command was updated to display MPLS VPN nonstop forwarding information.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router. The display output was modified to indicate whether BGP Nonstop Routing (NSR) with stateful switchover (SSO) is enabled and the reason the last BGP lost SSO capability.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA, and the output was modified to support per-VRF assignment of the BGP router ID.
12.2(31)SB2	The output was modified to support per-VRF assignment of the BGP router ID.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH, and the output was modified to support per-VRF assignment of the BGP router ID. **Note** In Cisco IOS Release 12.2(33)SXH, the command output does not display on the standby route processor in NSF/SSO mode.
12.4(20)T	The output was modified to support per-VRF assignment of the BGP router ID.
15.0(1)M	This command was modified. The output was modified to support BGP Event-Based VPN Import.
12.2(33)SRE	This command was modified. The command output was modified to support the BGP Event-Based VPN Import, BGP best external and BGP additional path features.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.

Release	Modification
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.

Usage Guidelines

Use this command to display VPNv4 information from the BGP database. The **show ip bgp vpnv4 all** command displays all available VPNv4 information. The **show ip bgp vpnv4 all summary** command displays BGP neighbor status. The **show ip bgp vpnv4 all labels** command displays explicit-null label information.

Examples

The following example shows all available VPNv4 information in a BGP routing table:

```
Router# show ip bgp vpnv4 all

BGP table version is 18, local router ID is 10.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP,? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:101 (default for vrf vpn1)
*>i10.6.6.6/32      10.0.0.21                11    100      0 ?
*> 10.7.7.7/32      10.150.0.2               11          32768 ?
*>i10.69.0.0/30     10.0.0.21                 0    100      0 ?
*> 10.150.0.0/24    0.0.0.0                   0          32768 ?
```

Table 30 describes the significant fields shown in the display.

Table 61 show ip bgp vpnv4 all Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows how to display a table of labels for NLRI prefixes that have a route distinguisher value of 100:1.

```
Router# show ip bgp vpnv4 rd 100:1 labels

Network            Next Hop       In label/Out label
Route Distinguisher: 100:1 (vrf1)
   10.0.0.0         10.20.0.60      34/nolabel
   10.0.0.0         10.20.0.60      35/nolabel
   10.0.0.0         10.20.0.60      26/nolabel
                    10.20.0.60      26/nolabel
   10.0.0.0         10.15.0.15      nolabel/26
```

Table 62 describes the significant fields shown in the display.

Table 62 show ip bgp vpnv4 rd labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Specifies the BGP next hop address.
In label	Displays the label (if any) assigned by this router.
Out label	Displays the label assigned by the BGP next-hop router.

The following example shows VPNv4 routing entries for the VRF named vpn1:

```
Router# show ip bgp vpnv4 vrf vpn1

BGP table version is 18, local router ID is 10.14.14.14
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
Route Distinguisher: 100:1 (default for vrf test1)
*> 10.1.1.1/32      192.168.1.1              0             0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
*> 10.2.2.2/32      192.168.1.1                            0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
*> 172.16.1.0/24    192.168.1.1              0             0 100 i
* i                 10.4.4.4                 0    100      0 100 i
r> 192.168.1.0      192.168.1.1              0             0 100 i
rbi                 10.4.4.4                 0    100      0 100 i
*> 192.168.3.0      192.168.1.1                            0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
```

Table 63 describes the significant fields shown in the display.

Table 63 show ip bgp vpnv4 vrf Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows attributes for network 192.168.9.0 that include multipaths, best path, and a recursive-via-host flag:

```
Router# show ip bgp vpnv4 vrf vpn1 192.168.9.0 255.255.255.0

BGP routing table entry for 100:1:192.168.9.0/24, version 44
Paths: (2 available, best #2, table test1)
  Additional-path
  Advertised to update-groups:
     2
  100, imported path from 400:1:192.168.9.0/24
    10.8.8.8 (metric 20) from 10.5.5.5 (10.5.5.5)
```

```
    Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
    Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
    Originator: 10.8.8.8, Cluster list: 10.5.5.5 , recursive-via-host
    mpls labels in/out nolabel/17
100, imported path from 300:1:192.168.9.0/24
  10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)
    Origin IGP, metric 0, localpref 100, valid, internal, best
    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 nolabel/17
```

Table 64 describes the significant fields shown in the display.

Table 64 show ip bgp vpnv4 all 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.
Multipath	Indicates the maximum paths configured (iBGP or eBGP).
Advertised to non peer-group peers	IP address of the BGP peers to which the specified route is advertised.
10.22.7.8 (metric 11) from 10.11.3.4 (10.0.0.8)	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	If shown, 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 100.
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.
multipath	One of multiple paths to the specified network.
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.

The following example shows routes that BGP could not install in the VRF table:

```
Router# show ip bgp vpnv4 vrf xyz rib-failure

Network            Next Hop                      RIB-failure   RIB-NH Matches
Route Distinguisher: 2:2 (default for vrf bar)
10.1.1.2/32        10.100.100.100      Higher admin distance              No
10.111.111.112/32  10.9.9.9            Higher admin distance             Yes
```

Table 53 describes the significant fields shown in the display.

Table 65 show ip bgp vpnv4 vrf rib-failure Field Descriptions

Field	Description
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
RIB-failure	Cause of the Routing Information Base (RIB) failure. Higher admin distance means that a route with a better (lower) administrative distance, such as a static route, already exists in the IP routing table.
RIB-NH Matches	Route status that applies only when Higher admin distance appears in the RIB-failure column and the **bgp suppress-inactive** command is configured for the address family being used. There are three choices: • Yes—Means that the route in the RIB has the same next hop as the BGP route or that the next hop recurses down to the same adjacency as the BGP next hop. • No—Means that the next hop in the RIB recurses down differently from the next hop of the BGP route. • n/a—Means that the **bgp suppress-inactive** command is not configured for the address family being used.

The following example shows the information displayed on the active and standby Route Processors when they are configured for NSF/SSO: MPLS VPN.

Note In Cisco IOS Release 12.2(33)SXH, the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature incurred various infrastructure changes. The result of those changes affects the output of this command on the standby Route Processor (RP). In Cisco IOS Release 12.2(33)SXH, the standby RP does not display any output from the **show ip bgp vpnv4** command.

Active Route Processor

```
Router# show ip bgp vpnv4 all labels

Network         Next Hop   In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32  0.0.0.0    16/aggregate(vpn1)
10.0.0.0/8      0.0.0.0    17/aggregate(vpn1)
Route Distinguisher: 609:1 (vpn0)
10.13.13.13/32  0.0.0.0    18/aggregate(vpn0)

Router# show ip bgp vpnv4 vrf vpn1 labels
```

```
Network          Next Hop   In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32   0.0.0.0    16/aggregate(vpn1)
10.0.0.0/8       0.0.0.0    17/aggregate(vpn1)
```

Standby Route Processor

```
Router# show ip bgp vpnv4 all labels

Network       Masklen   In label
Route Distinguisher: 100:1
10.12.12.12   /32       16
10.0.0.0      /8        17
Route Distinguisher: 609:1
10.13.13.13   /32       18

Router# show ip bgp vpnv4 vrf vpn1 labels

Network        Masklen   In label
Route Distinguisher: 100:1
10.12.12.12    /32       16
10.0.0.0       /8        17
```

Table 66 describes the significant fields shown in the display.

Table 66 show ip bgp vpn4 labels Field Descriptions

Field	Description
Network	The network address from the BGP table.
Next Hop	The BGP next-hop address.
In label	The label (if any) assigned by this router.
Out label	The label assigned by the BGP next-hop router.
Masklen	The mask length of the network address.

The following example displays output, including the explicit-null label, from the **show ip bgp vpnv4 all labels** command on a CSC-PE router:

```
Router# show ip bgp vpnv4 all labels

   Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (v1)
   10.0.0.0/24       10.0.0.0        19/aggregate(v1)
   10.0.0.1/32       10.0.0.0        20/nolabel
   10.1.1.1/32       10.0.0.0        21/aggregate(v1)
   10.10.10.10/32    10.0.0.1        25/exp-null
   10.168.100.100/32
                     10.0.0.1        23/exp-null
   10.168.101.101/32
                     10.0.0.1        22/exp-null
```

Table 67 describes the significant fields shown in the display.

Table 67 show ip bgp vpnv4 all labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
In label	Displays the label (if any) assigned by this router.
Out label	Displays the label assigned by the BGP next-hop router.
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.

The following example displays separate router IDs for each VRF in the output from an image in Cisco IOS Release 12.2(31)SB2, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, Cisco IOS XE Release 2.1, and later releases with the Per-VRF Assignment of BGP Router ID feature configured. The router ID is shown next to the VRF name.

```
Router# show ip bgp vpnv4 all

BGP table version is 5, 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
Route Distinguisher: 1:1 (default for vrf vrf_trans) VRF Router ID 10.99.1.2
*> 192.168.4.0      0.0.0.0                  0         32768 ?
Route Distinguisher: 42:1 (default for vrf vrf_user) VRF Router ID 10.99.1.1
*> 192.168.5.0      0.0.0.0                  0         32768 ?
```

Table 68 describes the significant fields shown in the display.

Table 68 show ip bgp vpnv4 all (VRF Router ID) Field Descriptions

Field	Description
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.
vrf	Name of the VRF.
VRF Router ID	Router ID for the VRF.

In this example, the BGP Event-Based VPN Import feature is configured in Cisco IOS Release 15.0(1)M, 12.2(33)SRE, and later releases. When the **import path selection** command is configured, but the **strict** keyword is not included, then a safe import path selection policy is in effect. When a path is imported as the best available path (when the bestpath or multipaths are not eligible for import), the imported path includes the wording “imported safety path,” as shown in the output.

```
Router# show ip bgp vpnv4 all 172.17.0.0

BGP routing table entry for 45000:1:172.17.0.0/16, version 10
Paths: (1 available, best #1, table vrf-A)
Flag: 0x820
   Not advertised to any peer
   2, imported safety path from 50000:2:172.17.0.0/16
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 200, localpref 100, valid, internal, best
```

```
      Extended Community: RT:45000:100
```

In this example the BGP Event-Based VPN Import feature is configured in Cisco IOS Release 15.0(1)M, 12.2(33)SRE, and later releases. When the **import path selection** command is configured with the **all** keyword, any path that matches an RD of the specified VRF will be imported, even though the path does not match the RTs imported by the specified VRF. In this situation, the imported path is marked as "not-in-vrf" as shown in the output. Note that on the net for vrf-A, this path is not the bestpath as any paths that are not in the VRFs appear less attractive than paths in the VRF.

```
Router# show ip bgp vpnv4 all 172.17.0.0

BBGP routing table entry for 45000:1:172.17.0.0/16, version 11
Paths: (2 available, best #2, table vrf-A)
Flag: 0x820
   Not advertised to any peer
   2
     10.0.101.2 from 10.0.101.2 (10.0.101.2)
       Origin IGP, metric 100, localpref 100, valid, internal, not-in-vrf
       Extended Community: RT:45000:200
       mpls labels in/out nolabel/16
   2
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 50, localpref 100, valid, internal, best
       Extended Community: RT:45000:100
       mpls labels in/out nolabel/16
```

Related Commands

Command	Description
import path limit	Specifies the maximum number of BGP paths, per VRF importing net, that can be imported from an exporting net.
import path selection	Specifies the BGP import path selection policy for a specific VRF instance.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

show ip bgp vpnv4 all dampening

To display BGP dampening information for the Virtual Private Network Version 4 (VPNv4) address family, use the **show ip bgp vpnv4 all dampening** command in user EXEC or privileged EXEC mode.

show ip bgp vpnv4 all dampening {dampened-paths | **flap-statistics [***network-address* **[***mask* | **bestpath** | **multipaths**] | *ip-prefix/length* | **cidr-only** | **filter-list** *filter-list* | **oer-paths** | **prefix-list** *prefix-list* | **quote-regexp** *regexp* | **regexp** *regexp* | **route-map** *map-name* | **version** {*number* | **recent** }] | **parameters**}

Syntax Description

dampened-paths	Display routes suppressed due to dampening.
flap-statistics	Displays flap statistics of routes.
network-address	(Optional) Used with the **flap-statistics** keyword, network in the BGP routing table to display.
mask	(Optional) Used with the *network-address* argument, network mask that determines the networks displayed.
bestpath	(Optional) Used with the *network-address* argument, displays the bestpath for this prefix.
multipaths	(Optional) Used with the *network-address* argument, displays the multipaths for this prefix.
ip-prefix/length	(Optional) Used with the **flap-statistics** keyword, IP prefix/network length, such as 10.0.0.0/8.
cidr-only	(Optional) Used with the **flap-statistics** keyword, displays only routes with non-natural netmasks.
filter-list *filter-list*	(Optional) Used with the **flap-statistics** keyword, displays routes that conform to the specified filter list in the range 1-500.
oer-paths	(Optional) Used with the **flap-statistics** keyword, displays all OER controlled paths.
prefix-list *prefix-list*	(Optional) Used with the **flap-statistics** keyword, displays routes allowed by the prefix list.
quote-regexp *regexp*	(Optional) Used with the **flap-statistics** keyword, displays routes matching the AS path “regular expression”.
regexp *regexp*	(Optional) Used with the **flap-statistics** keyword, displays routes matching the AS path regular expression.
route-map *map-name*	(Optional) Used with the **flap-statistics** keyword, displays routes allowed by the route map.
version *number* | **recent**	(Optional) Used with the **flap-statistics** keyword, displays version of BGP table.
parameters	Display details of configured dampening parameters.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use this command to display dampening information for the VPNv4 address family.

Examples

The following example shows dampening flap-statistics for the VPNv4 address family:

```
Router# show ip bgp vpnv4 all dampening flap-statistics

For_address_family: VPNv4 Unicast

% dampening not enabled for base

For vrf: Cust_A

BGP table version is 15, local router ID is 144.124.23.2
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, f
RT-Filter
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          From            Flaps Duration Reuse    Path
*>  20.20.20.20/32   172.16.1.2      1     00:01:05          65001

For vrf: Cust_B

*d  11.11.11.11/32   192.168.1.2     3     00:04:22 00:04:49 65001
Router#
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes BGP route dampening parameters.

show ip bgp vpnv6 unicast all dampening

To display BGP dampening information for the Virtual Private Network Version 6 (VPNv6) address family, use the **show ip bgp vpnv6 unicast all dampening** command in user EXEC or privileged EXEC mode.

show ip bgp vpnv6 unicast all dampening {**dampened-paths** | **flap-statistics** [*network/length* | **filter-list** *filter-list* | **injected-paths** | **prefix-list** *prefix-list* | **quote-regexp** *regexp* | **regexp** *regexp* | **route-map** *map-name*] | **parameters**}

Syntax Description

dampened-paths	Display routes suppressed due to dampening.
flap-statistics	Displays flap statistics of routes.
network/length	(Optional) Used with the **flap-statistics** keyword, IPv6 prefix network/length in the format *X:X:X:X::X/<0-128>*.
filter-list *filter-list*	(Optional) Used with the **flap-statistics** keyword, displays routes that conform to the specified filter list in the range 1-500.
injected-paths	(Optional) Used with the **flap-statistics** keyword, displays all injected paths.
prefix-list *list*	(Optional) Used with the **flap-statistics** keyword, displays routes allowed by the prefix list.
quote-regexp *regexp*	(Optional) Used with the **flap-statistics** keyword, displays routes matching the AS path “regular expression”.
regexp *regexp*	(Optional) Used with the **flap-statistics** keyword, displays routes matching the AS path regular expression.
route-map *map-name*	(Optional) Used with the **flap-statistics** keyword, displays routes allowed by the route map.
parameters	Display details of configured dampening parameters.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

Use this command to display BGP dampening information for the VPNv6 address family.

Examples

The following example shows dampening VPNv6 information:

```
Router# show ip bgp vpnv6 unicast all dampening flap-statistics

For_address_family: VPNv6 Unicast

% dampening not enabled for base
```

```
For vrf: RED


For vrf: BLUE

BGP table version is 36, local router ID is 10.0.0.1
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, f
RT-Filter
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          From            Flaps Duration Reuse    Path
*d  11::/64          20::2           3     00:03:17 00:05:59 2
*d  22::/64          20::2           3     00:03:17 00:05:59 2
*d  33::/64          20::2           3     00:03:17 00:05:59 2
*d  44::/64          20::2           3     00:03:17 00:05:59 2
*d  55::/64          20::2           3     00:03:17 00:05:59 2
R1#
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes BGP route dampening parameters.

show ip community-list

To display configured community lists, use the **show ip community-list** command in user or privileged EXEC mode.

show ip community-list [*community-list-number* | *community-list-name*] [**exact-match**]

Syntax Description

community-list-number	(Optional) A standard or expanded community list number in the range from 1 to 500.
community-list-name	(Optional) Community list name. The community list name can be standard or expanded.
exact-match	(Optional) Displays only routes that have an exact match.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(10)S	Named community list support was added.
12.0(16)ST	Named community lists support was integrated into Cisco IOS Release 12.0(16)ST.
12.1(9)E	Named community lists support was integrated into Cisco IOS Release 12.1(9)E.
12.2(8)T	Named community lists support was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command can be used without any arguments or keywords. If no arguments are specified, this command will display all community lists. However, the community list name or number can be specified when entering the **show ip community-list** command. This option can be useful for filtering the output of this command and verifying a single named or numbered community list.

Examples

The following sample output is similar to the output that will be displayed when the **show ip community-list** command is entered in privileged EXEC mode:

```
Router# show ip community-list

Community standard list 1
     permit 3
```

```
     deny 5
Community (expanded) access list 101
    deny 4
    permit 6
Named Community standard list COMMUNITY_LIST_NAME
    permit 1
    deny 7
Named Community expanded list COMMUNITY_LIST_NAME_TWO
    deny 2
    permit 8
```

Table 69 describes the significant fields shown in the display.

Table 69 show ip community-list Field Descriptions

Field	Description
Community standard list	If shown, this value will display a standard community list number (1 to 99). The standard community list number will immediately follow this value.
Community (expanded) access list	If shown, this value will display an expanded community list number (100 to 500). The expanded community list number will immediately follow this value.
Named community standard list	If shown, this value will display a standard community list name. The standard community list name will immediately follow this value.
Named community expanded list	If shown, this value will display an expanded community list name. The expanded community list name will immediately follow this value.

show ip extcommunity-list

To display routes that are permitted by an extended community list, use the **show ip extcommunity-list** command in user EXEC or privileged EXEC mode.

show ip extcommunity-list [*list-number* | *list-name*]

Syntax Description

list-number	(Optional) Specifies an extended community list number from 1 to 500. A standard extended community list number is from 1 to 99. An expanded extended list is from 100 to 500.
list-name	(Optional) Specifies an extended community list name. If a specific extended community list number is not specified, all locally configured extended community lists will be displayed by default.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1	This command was introduced.
12.2(25)S	Support for named extended community lists was added. Minor formatting changes were made to the output.
12.3(11)T	Support for named extended community lists was added. Minor formatting changes were made to the output.
12.2(27)SBC	This command was integrated into the Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.

Release	Modification
12.2(33)SRE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

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 the route target—RT in the output—contains a 4-byte autonomous system number as part of the extended community list, it will be displayed in the appropriate format.

Examples

The following is sample output from the **show ip extcommunity-list** command:

```
Router# show ip extcommunity-list

Standard extended community-list 1
     10 permit RT:64512:10
     20 permit SoO:65400:20
     30 deny RT:65424:30 SoO:64524:40
Standard extended community-list 99
     10 permit RT:65504:40 SoO:65505:50
     20 deny RT:65406:60 SoO:65307:70
Expanded extended community-list LIST_NAME
     10 permit 0-9* A-Z* a-z*
```

Table 70 describes the significant fields shown in the display.

Table 70 show ip extcommunity-list Field Descriptions

Field	Description
... extended community-list....	The type of extended community-list (standard or expanded), and the name or number of the extended community list.
10	The sequence number of the extended community list entry. 10 is the lowest default sequence number. Extended community lists increment by 10 when default values are configured.
permit/deny	Indicates a permit or deny sequence entry.

Table 70 show ip extcommunity-list Field Descriptions (continued)

Field	Description
RT/SoO	Indicates the route target or the site of origin used in a standard extended community list.
0-9* A-Z* a-z*	Regular expression used in an expanded extended community list.

The following output is from the **show ip extcommunity-list** command after a 4-byte autonomous system number has been configured as part of the route target. The 4-byte autonomous system number, 65537, is displayed in the default asplain format. 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# show ip extcommunity-list 1

Extended community standard list 1
     permit RT:65537:100
```

The following output displays a 4-byte autonomous system number that has been configured as part of the route target. The 4-byte autonomous system number—1.1—is displayed in asdot notation. The dot notation is the only format for 4-byte autonomous system numbers in Cisco IOS Release 12.0(32)S12, 12.4(24)T, or Cisco IOS XE Release 2.3. This output can also be seen 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, or later releases. after the **bgp asnotation dot** command has been entered to display 4-byte autonomous system numbers in dot notation.

```
Router# show ip extcommunity-list 1

Extended community standard list 1
     permit RT:1.1:100
```

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.
router bgp	Configures the BGP routing process.
show route-map	Displays configured route maps.

show ip policy-list

To display information about a configured policy list and policy list entries, use the **show ip policy-list command in user** EXEC mode.

show ip policy-list [*policy-list-name*]

Syntax Description

policy-list-name	(Optional) Displays information about the specified policy list with this argument.

Command Modes

EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into 12.2(15)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ip policy-list** command. The output of this command will display the policy-list name and configured match clauses. The following sample output is similar to the output that will be displayed:

```
Router> show ip policy-list

policy-list POLICY-LIST-NAME-1 permit
  Match clauses:
    metric 20
policy-list POLICY-LIST-NAME-2 permit
  Match clauses:
    as-path (as-path filter): 1
```

Related Commands

Command	Description
show route-map	Displays configured route maps and information about referenced policy maps.

show ip prefix-list

To display information about a prefix list or prefix list entries, use the **show ip prefix-list** command in user or privileged EXEC mode.

show ip prefix-list [**detail** | **summary**][*prefix-list-name* [**seq** *sequence-number* | *network/length* [**longer**| **first-match**]]]

Syntax Description

detail | **summary**	(Optional) Displays detailed or summarized information about all prefix lists.
prefix-list-name	(Optional) Displays the entries in a specific prefix list.
seq *sequence-number*	(Optional) Displays only the prefix list entry with the specified sequence number in the specified prefix-list.
network/length	(Optional) Displays all entries in the specified prefix list that use this network address and netmask length (in bits).
longer	(Optional) Displays all entries of the specified prefix list that match or are more specific than the given *network/length.*
first-match	(Optional) Displays the first entry of the specified prefix list that matches the given *network/length*.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows the output of the **show ip prefix-list** command with details about the prefix list named test:

```
Router# show ip prefix-list detail test

ip prefix-list test:
Description: test-list
 count: 1, range entries: 0, sequences: 10 - 10, refcount: 3
 seq 10 permit 10.0.0.0/8 (hit count: 0, refcount: 1)
```

Related Commands

Command	Description
clear ip prefix-list	Resets the hit count of the prefix list entries.
distribute-list in (BGP)	Filters networks received in updates.

distribute-list out (BGP)	Suppresses networks from being advertised in updates.
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list description	Adds a text description of a prefix list.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.

show ip route

To display the current state of the routing table, use the **show ip route** command in user EXEC or privileged EXEC mode.

show ip route [*ip-address* [**repair-paths** | **next-hop-override** [**dhcp**] | *mask* [**longer-prefixes**]] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*] | **static download** | **update-queue**]

Syntax Description

ip-address	(Optional) IP address about which routing information should be displayed.
repair-paths	(Optional) Displays the repair paths.
next-hop-override	(Optional) Displays the Next Hop Resolution Protocol (NHRP) overrides associated with a particular route, along with the corresponding default next hops.
dhcp	(Optional) Displays routes added by the Dynamic Host Configuration Protocol (DHCP) server.
mask	(Optional) The subnet mask.
longer-prefixes	(Optional) Specifies that only routes matching the *ip-address* and *mask* pair should be displayed.
protocol	(Optional) The name of a routing protocol, or the keyword **connected**, **mobile**, **static**, or **summary**. If you specify a routing protocol, use one of the following keywords: **bgp**, **eigrp**, **hello**, **isis**, **odr**, **ospf**, **nhr**, and **rip**.
process-id	(Optional) The number used to identify a process of the specified protocol.
list	(Optional) Filters output by an access list name or number.
access-list-number	(Optional) Specific access list number for which output from the routing table should be displayed.
access-list-name	(Optional) Specific access list name for which output from the routing table should be displayed.
static	(Optional) Displays static routes.
download	(Optional) Displays the route installed using the authentication, authorization, and accounting (AAA) route download function. This keyword is used only when AAA is configured.
update-queue	(Optional) Displays Routing Information Base (RIB) queue updates.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
9.2	This command was introduced.
10.0	The “D—EIGRP, EX—EIGRP, N1—OSPF NSSA external type 1 route” and “N2—OSPF NSSA external type 2 route” codes were added to the command output.
10.3	The *process-id* argument was added.
11.0	The **longer-prefixes** keyword was added.
11.1	The “U—per-user static route” code was added to the command output.
11.2	The “o—on-demand routing” code was added to the command output.
12.2(33)SRA	This command was modified. The **update-queue** keyword was added.
11.3	The output from the **show ip route** *ip-address* command was enhanced to display the origination of an IP route in Intermediate System-to-Intermediate System (IS-IS) networks.
12.0(1)T	The “M—mobile” code was added to the command output.
12.0(3)T	The “P—periodic downloaded static route” code was added to the command output.
12.0(4)T	The “ia—IS-IS” code was added to the command output.
12.2(2)T	The output from the **show ip route** *ip-address* command was enhanced to display information on the multipaths to the specified network.
12.2(13)T	The *egp* and *igrp* arguments were removed because the exterior gateway protocol (EGP) and the Interior Gateway Routing Protocol (IGRP) are no longer available in Cisco IOS software.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.3(2)T	The output was enhanced to display route tag information.
12.3(8)T	The output was enhanced to display static routes using DHCP.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRE	This command was modified. The **dhcp** and **repair-paths** keywords were added. Support for the Border Gateway Protocol (BGP) best external and BGP additional path features was added.
12.2(24)T	This command was modified. The “L” code was added.
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 modified. The **next-hop-override** and **nhrp** keywords were added.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

The **show ip route static download** command provides a way to display all dynamic static routes with name and distance information, including active and inactive ones. You can display all active dynamic static routes with both the **show ip route** and **show ip route static** commands after these active routes are added in the main routing table.

Examples

Routing Table Examples

The following examples show the standard routing tables displayed by the **show ip route** command. Use the codes displayed at the beginning of each report and the information in Table 71 to understand the type of route.

The following is sample output from the **show ip route** command when entered without an address:

```
Router# show ip route

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is 10.119.254.240 to network 10.140.0.0

O E2 10.110.0.0 [160/5] via 10.119.254.6, 0:01:00, Ethernet2
E    10.67.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
O E2 10.68.132.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.130.0.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
E    10.128.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.129.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.65.129.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.10.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.75.139.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.16.208.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.84.148.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.31.223.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.44.236.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.141.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.140.0.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
```

The following is sample output that includes IS-IS Level 2 routes learned:

```
Router# show ip route

Codes: L- Local R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is 192.168.1.2 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 192.168.1.2
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.10.10.0/24 is directly connected, Vlan1
L        10.10.10.1/32 is directly connected, Vlan1
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/30 is directly connected, GigabitEthernet0
L        192.168.1.1/32 is directly connected, GigabitEthernet0
```

The following is sample output using the **longer-prefixes** keyword. When the **longer-prefixes** keyword is included, the address and mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed.

In the following example, the logical AND operation is performed on the source address 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 10.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Router# show ip route 10.0.0.0 10.0.0.0 longer-prefixes

Codes: L - Local R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.4.9.0/24 is directly connected, GigabitEthernet0/1
L        10.4.9.134/32 is directly connected, GigabitEthernet0/1
      171.69.0.0/16 is variably subnetted, 2 subnets, 2 masks
S        171.69.0.0/16 [1/0] via 10.4.9.1
S        171.69.1.129/32 [1/0] via 10.4.9.1
```

The following examples display all downloaded static routes. A P designates which route was installed using AAA route download.

```
Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR, P - periodic downloaded static route
       T - traffic engineered route

Gateway of last resort is 172.21.17.1 to network 0.0.0.0

        172.31.0.0/32 is subnetted, 1 subnets
P       172.31.229.41 is directly connected, Dialer1 20.0.0.0/24 is subnetted, 3 subnets
P       10.1.1.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.3.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.2.0 [200/0] via 172.31.229.41, Dialer1

Router# show ip route static

     172.27.4.0/8 is variably subnetted, 2 subnets, 2 masks
P       172.16.1.1/32 is directly connected, BRI0
P       172.27.4.0/8 [1/0] via 10.1.1.1, BRI0
S    172.31.0.0/16 [1/0] via 172.21.114.65, Ethernet0
S    10.0.0.0/8 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
     172.21.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.21.114.201/32 is directly connected, BRI0
S       172.21.114.205/32 is directly connected, BRI0
S       172.21.114.174/32 is directly connected, BRI0
S       172.21.114.12/32 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
P    10.1.0.0/16 is directly connected, BRI0
P    10.2.2.0/24 is directly connected, BRI0
S*   0.0.0.0/0 [1/0] via 172.21.114.65, Ethernet0
```

```
S    172.29.0.0/16 [1/0] via 172.21.114.65, Ethernet0
```

The following example shows how to use the **show ip route static download** command to display all active and inactive routes installed using AAA route download:

```
Router# show ip route static download

Connectivity: A - Active, I - Inactive

A     10.10.0.0 255.0.0.0 BRI0
A     10.11.0.0 255.0.0.0 BRI0
A     10.12.0.0 255.0.0.0 BRI0
A     10.13.0.0 255.0.0.0 BRI0
I     10.20.0.0 255.0.0.0 172.21.1.1
I     10.22.0.0 255.0.0.0 Serial0
I     10.30.0.0 255.0.0.0 Serial0
I     10.31.0.0 255.0.0.0 Serial1
I     10.32.0.0 255.0.0.0 Serial1
A     10.34.0.0 255.0.0.0 192.168.1.1
A     10.36.1.1 255.255.255.255 BRI0 200 name remote1
I     10.38.1.9 255.255.255.0 192.168.69.1
```

The following example shows how to use the **show ip route nhrp** command to enable shortcut switching on the tunnel interface:

```
Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP

Gateway of last resort is not set

       10.0.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Tunnel0
C       172.16.22.0 is directly connected, Ethernet1/0
H       172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
     10.11.0.0/24 is subnetted, 1 subnets
C       10.11.11.0 is directly connected, Ethernet0/0

Router# show ip route nhrp

H       172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
```

The following is sample output using the **next-hop-override** keyword. When the **next-hop-override** keyword is included, the NHRP Nexthop-overrides associated with a particular route, along with the corresponding default next hops, are displayed.

```
==============================================================
1) Initial configuration
==============================================================
Router# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
```

```
       + - replicated route

Gateway of last resort is not set

      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Router# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set

      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Router# show ip cef

Prefix              Next Hop            Interface
.
.
.
10.2.1.255/32        receive             Loopback1
10.10.10.0/24       attached            Tunnel0  <<<<<<<<
10.11.11.0/24       attached            Ethernet0/0
127.0.0.0/8         drop
.
.
.
================================================================
2) Add a Nexthop-override
    address = 10.10.10.0
    mask = 255.255.255.0
    gateway = 10.1.1.1
    interface = Tunnel0
================================================================
Router# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route
```

```
Gateway of last resort is not set

      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
% S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Router# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set

      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
% S        10.10.10.0 is directly connected, Tunnel0
                  [NHO][1/0] via 10.1.1.1, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Router# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback110.10.10.0/24

10.10.10.0/24       10.1.1.1             Tunnel0
10.11.11.0/24       attached            Ethernet0/0
10.12.0.0/16 drop
.
.
.

================================================================
3) Delete a Nexthop-override
    address = 10.10.10.0
    mask = 255.255.255.0
    gateway = 10.11.1.1
    interface = Tunnel0
================================================================
Router# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route
```

```
Gateway of last resort is not set

      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Router# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set

      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Router# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback110.10.10.0/24

10.10.10.0/24        attached             Tunnel0
10.11.11.0/24        attached             Ethernet0/0
10.120.0.0/16 drop
.
.
.
```

Table 71 show ip route Field Descriptions

Field	Description
Codes	Indicates the protocol that derived the route. It can be one of the following values: • B—BGP derived • C—connected • D—Enhanced Interior Gateway Routing Protocol (EIGRP) • EX—EIGRP external • H— NHRP • i—IS-IS derived • ia—IS-IS • L—local • M—mobile • O—Open Shortest Path First (OSPF) derived • P—periodic downloaded static route • R—Routing Information Protocol (RIP) derived • S—static • U—per-user static route • o—on-demand routing • +—replicated route
Codes	Type of route. It can be one of the following values: • *—Indicates the last path used when a packet was forwarded. It pertains only to the nonfast-switched packets. However, it does not indicate which path will be used next when forwarding a nonfast-switched packet, except when the paths are equal cost. • E1—OSPF external type 1 route • E2—OSPF external type 2 route • IA—OSPF inter area route • L1—IS-IS Level 1 route • L2—IS-IS Level 2 route • N1—OSPF not-so-stubby area (NSSA) external type 1 route • N2—OSPF NSSA external type 2 route
10.110.0.0	Indicates the address of the remote network.
[160/5]	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.119.254.6	Specifies the address of the next router to the remote network.
0:01:00	Specifies the last time the route was updated (in hours:minutes:seconds).
Ethernet2	Specifies the interface through which the specified network can be reached.

Specific Route Information

When you specify that you want information about a specific network displayed, more detailed statistics are shown. The following is sample output from the **show ip route** command when entered with the IP address 10.0.0.1:

```
Router# show ip route 10.0.0.1

Routing entry for 10.0.0.1/32
    Known via “isis”, distance 115, metric 20, type level-1
    Redistributing via isis
    Last update from 10.191.255.251 on Fddi1/0, 00:00:13 ago
    Routing Descriptor Blocks:
    * 10.22.22.2, from 10.191.255.247, via Serial2/3
       Route metric is 20, traffic share count is 1
       10.191.255.251, from 10.191.255.247, via Fddi1/0
       Route metric is 20, traffic share count is 1
```

When an IS-IS router advertises its link-state information, it includes one of its own IP addresses to be used as the originator IP address. When other routers calculate IP routes, they can store the originator IP address with each route in the routing table.

The preceding example shows the output from the **show ip route** command for an IP route generated by IS-IS. Each path that is shown under the Routing Descriptor Blocks report displays two IP addresses. The first address (10.22.22.2) is the next hop address. The second is the originator IP address from the advertising IS-IS router. This address helps you determine where a particular IP route has originated in your network. In the example the route to 10.0.0.1/32 was originated by a router with IP address 10.191.255.247.

Table 72 describes the significant fields shown when using the **show ip route** command with an IP address.

Table 72 show ip route with IP Address Field Descriptions

Field	Description
Routing entry for 10.0.0.1/32	Network number and mask.
Known via...	Indicates how the route was derived.
Tag	Integer that is used to implement the route.
type	Indicates the IS-IS route type (Level 1 or Level 2).
Redistributing via...	Indicates the redistribution protocol.
Last update from 10.191.255.251	Indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived.
Routing Descriptor Blocks:	Displays the next hop IP address followed by the information source.
Route metric	This value is the best metric for this routing descriptor block.
traffic share count	Number of uses for this routing descriptor block.

The following is sample output using the **longer-prefixes** keyword. When the **longer-prefixes** keyword is included, the address and mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed.

In the following example, the logical AND operation is performed on the source address 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 10.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Router# show ip route 10.0.0.0 10.0.0.0 longer-prefixes

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is not set

S    10.134.0.0 is directly connected, Ethernet0
S    10.10.0.0 is directly connected, Ethernet0
S    10.129.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
S    10.49.246.0 is directly connected, Ethernet0
S    10.160.97.0 is directly connected, Ethernet0
S    10.153.88.0 is directly connected, Ethernet0
S    10.76.141.0 is directly connected, Ethernet0
S    10.75.138.0 is directly connected, Ethernet0
S    10.44.237.0 is directly connected, Ethernet0
S    10.31.222.0 is directly connected, Ethernet0
S    10.16.209.0 is directly connected, Ethernet0
S    10.145.0.0 is directly connected, Ethernet0
S    10.141.0.0 is directly connected, Ethernet0
S    10.138.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
     10.19.0.0 255.255.255.0 is subnetted, 1 subnets
C       10.19.64.0 is directly connected, Ethernet0
     10.69.0.0 is variably subnetted, 2 subnets, 2 masks
C       10.69.232.32 255.255.255.240 is directly connected, Ethernet0
S       10.69.0.0 255.255.0.0 is directly connected, Ethernet0
```

The following output includes the tag 120 applied to the route 10.22.0.0/16. You must specify an IP prefix in order to see the tag value.

```
Router# show ip route 10.22.0.0

Routing entry for 10.22.0.0/16
  Known via “isis”, distance 115, metric 12
  Tag 120, type level-1
  Redistributing via isis
  Last update from 172.19.170.12 on Ethernet2, 01:29:13 ago
  Routing Descriptor Blocks:
    * 172.19.170.12, from 10.3.3.3, via Ethernet2
        Route metric is 12, traffic share count is 1
        Route tag 120
```

Static Routes Using a DHCP Gateway Examples

The following example shows that IP route 10.8.8.0 is directly connected to the Internet and is the next-hop (option 3) default gateway. Routes 10.1.1.1 [1/0], 10.3.2.1 [24/0], and 172.2.2.2 [1/0] are static, and route 10.0.0.0/0 is a default route candidate.

```
Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.19.14 to network 0.0.0.0

10.0.0.0/24 is subnetted, 1 subnets
C 10.8.8.0 is directly connected, Ethernet1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.1.1.1 [1/0] via 10.8.8.1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.3.2.1 [24/0] via 10.8.8.1
  172.16.0.0/32 is subnetted, 1 subnets
S 172.2.2.2 [1/0] via 10.8.8.1
  10.0.0.0/28 is subnetted, 1 subnets
C 10.0.19.0 is directly connected, Ethernet0
  10.0.0.0/24 is subnetted, 1 subnets
C 10.15.15.0 is directly connected, Loopback0

S* 10.0.0.0/0 [1/0] via 10.0.19.14
```

The following sample output from the **show ip route repair-paths** command shows the repair paths marked with the tag [RPR]:

```
Router# show ip route repair-paths

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/32 is subnetted, 3 subnets
C        10.1.1.1 is directly connected, Loopback0
B        10.2.2.2 [200/0] via 172.16.1.2, 00:31:07
                  [RPR][200/0] via 192.168.1.2, 00:31:07
B        10.9.9.9 [20/0] via 192.168.1.2, 00:29:45
                  [RPR][20/0] via 192.168.3.2, 00:29:45
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/0
L        172.16.1.1/32 is directly connected, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Serial2/0
L        192.168.1.1/32 is directly connected, Serial2/0
B     192.168.3.0/24 [200/0] via 172.16.1.2, 00:31:07
                     [RPR][200/0] via 192.168.1.2, 00:31:07
B     192.168.9.0/24 [20/0] via 192.168.1.2, 00:29:45
                     [RPR][20/0] via 192.168.3.2, 00:29:45
B     192.168.13.0/24 [20/0] via 192.168.1.2, 00:29:45
                      [RPR][20/0] via 192.168.3.2, 00:29:45

Router# show ip route repair-paths 10.9.9.9

>Routing entry for 10.9.9.9/32
>  Known via "bgp 100", distance 20, metric 0
>  Tag 10, type external
```

```
>  Last update from 192.168.1.2 00:44:52 ago
>  Routing Descriptor Blocks:
>  * 192.168.1.2, from 192.168.1.2, 00:44:52 ago, recursive-via-conn
>      Route metric is 0, traffic share count is 1
>      AS Hops 2
>      Route tag 10
>      MPLS label: none
>    [RPR]192.168.3.2, from 172.16.1.2, 00:44:52 ago
>      Route metric is 0, traffic share count is 1
>      AS Hops 2
>      Route tag 10
>      MPLS label: none
```

Related Commands

Command	Description
show dialer	Displays general diagnostic information for interfaces configured for DDR.
show interfaces tunnel	Displays a list of tunnel interface information.
show ip route summary	Displays the current state of the routing table in summary format.

show ip route vrf

To display the IP routing table associated with a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **show ip route vrf** command in user EXEC or privileged EXEC mode.

show ip route vrf *vrf-name* [**connected**] [*protocol* [*as-number*] [*tag*] [*output-modifiers*]] [**list** *number* [*output-modifiers*]] [**profile**] [**static** [*output-modifiers*]] [**summary** [*output-modifiers*]] [**supernets-only** [*output-modifiers*]] [*ip-address* [**repair-paths** [**dhcp** | *mask* [**longer-prefixes**]]]] [**supernets-only**]

Syntax Description

vrf-name	Name assigned to the VRF.
connected	(Optional) Displays all connected routes in a VRF.
protocol	(Optional) To specify a routing protocol, use one of the following keywords: **bgp**, **egp**, **eigrp**, **hello**, **igrp**, **isis**, **ospf**, or **rip**.
as-number	(Optional) Autonomous system number.
tag	(Optional) Cisco IOS routing area label.
output-modifiers	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
ip-prefix	(Optional) Specifies a network to display.
list *number*	(Optional) Specifies the IP access list to display.
profile	(Optional) Displays the IP routing table profile.
static	(Optional) Displays static routes.
summary	(Optional) Displays a summary of routes.
ip-address	(Optional) Address about which routing information should be displayed.
repair-paths	(Optional) Displays the repair paths.
dhcp	(Optional) Displays routes added by the DHCP server.
longer-prefixes	(Optional) Specifies that only routes matching the *ip-address* and *mask* pair should be displayed.
supernets-only	(Optional) Displays supernet entries only.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(2)T	The *ip-prefix* argument was added. The output from the **show ip route vrf** *vrf-name ip-prefix* command was enhanced to display information on the multipaths to the specified network.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	Enhanced Interior Gateway Routing Protocol (EIGRP) VRF support was added.

Release	Modification
12.2(15)T	EIGRP VRF support was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	EIGRP VRF support 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.
12.2(33)SXH	The output was enhanced to display remote label information and corresponding MPLS flags for prefixes that have remote labels stored in the Routing Information Base (RIB).
12.2(33)SRE	This command was modified. The **repair-paths**, **dhcp**, and **supernets-only** keywords were added. Support for the BGP best external and BGP additional path features was added.
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.

Usage Guidelines

This command displays specified information from the IP routing table of a VRF.

Examples

This example shows the IP routing table associated with the VRF named vrf1:

```
Router# show ip route vrf vrf1

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
       T - traffic engineered route

Gateway of last resort is not set

B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:19
C    10.0.0.0/8 is directly connected, Ethernet1/3
B    10.0.0.0/8 [20/0] via 10.0.0.1, 02:10:22
B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:20
```

This example shows BGP entries in the IP routing table associated with the VRF named vrf1:

```
Router# show ip route vrf vrf1 bgp

B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:44:14
B  10.0.0.0/8 [20/0] via 10.0.0.1, 03:44:12
B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:43:14
```

This example shows the IP routing table associated with a VRF named PATH and network 10.22.22.0:

```
Router# show ip route vrf PATH 10.22.22.0

Routing entry for 10.22.22.0/24
  Known via "bgp 1", distance 200, metric 0
  Tag 22, type internal
  Last update from 10.22.5.10 00:01:07 ago
  Routing Descriptor Blocks:
  * 10.22.7.8 (Default-IP-Routing-Table), from 10.11.3.4, 00:01:07 ago
```

```
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.22.1.9 (Default-IP-Routing-Table), from 10.11.1.2, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.22.6.10 (Default-IP-Routing-Table), from 10.11.6.7, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.22.4.10 (Default-IP-Routing-Table), from 10.11.4.5, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.22.5.10 (Default-IP-Routing-Table), from 10.11.5.6, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
```

The following are sample outputs from the **show ip route vrf** command to include the recursive-via-host and recursive-via-connected flags.

```
Router# show ip route vrf v2 10.2.2.2

Routing Table: v2
Routing entry for 10.2.2.2/32
  Known via "bgp 10", distance 20, metric 0
  Tag 100, type external
  Last update from 192.168.1.1 00:15:54 ago
  Routing Descriptor Blocks:
  * 192.168.1.1, from 192.168.1.1, 00:15:54 ago, recursive-via-conn
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 100
      MPLS label: none

Router# show ip route vrf v2 10.2.2.2

Routing Table: v2
Routing entry for 10.2.2.2/32
  Known via "bgp 10", distance 200, metric 0
  Tag 100, type internal
  Last update from 10.3.3.3 00:18:11 ago
  Routing Descriptor Blocks:
  * 10.3.3.3 (default), from 10.5.5.5, 00:18:11 ago, recursive-via-host
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 100
      MPLS label: 16
      MPLS Flags: MPLS Required
```

Table 73 describes the significant fields shown when the **show ip route vrf** *vrf-name ip-prefix* command is used.

Table 73 show ip route vrf Field Descriptions

Field	Description
Routing entry for 10.22.22.0/24	Network number.
Known via ...	Indicates how the route was derived.
distance	Administrative distance of the information source.
metric	The metric to reach the destination network.
Tag	Integer that is used to implement the route.

Table 73 show ip route vrf Field Descriptions (continued)

Field	Description
type	Indicates that the route is an L1 type or L2 type route.
Last update from 10.22.5.10	Indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived.
00:01:07 ago	Specifies the last time the route was updated (in hours:minutes:seconds).
Routing Descriptor Blocks:	Displays the next hop IP address followed by the information source.
10.22.6.10, from 10.11.6.7, 00:01:07 ago	Indicates the next hop address, the address of the gateway that sent the update, and the time that has elapsed since this update was received (in hours:minutes:seconds).
Route metric	This value is the best metric for this routing descriptor block.
traffic share count	Number of uses for this routing descriptor block.
AS Hops	Number of hops to the destination or to the router where the route first enters internal BGP (iBGP).

Example of Output Using the Cisco IOS Software Modularity for Layer 3 VPNs Feature

The following is sample output from the **show ip route vrf** command on routers using the Cisco IOS Software Modularity for Layer 3 VPNs feature. The output includes remote label information and corresponding MPLS flags for prefixes that have remote labels stored in the RIB, if BGP is the label distribution protocol:

```
Router# show ip route vrf v2 10.2.2.2

Routing entry for 10.2.2.2/32
  Known via "bgp 1", distance 200, metric 0, type internal
  Redistributing via ospf 2
  Advertised by ospf 2 subnets
  Last update from 10.0.0.4 00:22:59 ago
  Routing Descriptor Blocks:
  * 10.0.0.4 (Default-IP-Routing-Table), from 10.0.0.31, 00:22:59 ago
      Route metric is 0, traffic share count is 1
      AS Hops 0
      MPLS label: 1300
      MPLS Flags: MPLS Required
```

Table 74 describes the significant fields shown in the display.

Table 74 show ip route vrf Field Descriptions

Field	Description
MPLS label	Displays the BGP prefix from the BGP peer. The output shows one of the following values: • A label value (16 - 1048575) • A reserved label value, such as explicit-null or implicit-null • The word “none” if no label is received from the peer The MPLS label field does not display if any of the following conditions is true: • BGP is not the LDP. However, OSPF prefixes learned via sham link display an MPLS label. • MPLS is not supported. • The prefix was imported from another VRF, where the prefix was an IGP prefix and LDP provided the remote label for it.
MPLS Flags	The name of one of the following MPLS flags is displayed if any is set: • MPLS Required—Packets are forwarded to this prefix because the MPLS label stack is present. If MPLS is disabled in the outgoing interface, the packets are dropped. • No Global—MPLS packets for this prefix are forwarded from the VRF interface, not from the interface in global table. Using the VRF interface prevents loops in scenarios that use ieBGP multipath. • NSF—The prefix is from an NSF-aware neighbor. If the routing information temporarily disappears due to a disruption in the control plane, packets for this prefix are preserved.

The following sample output from the **show ip route vrf** command shows the repair paths marked with the tag [RPR], the best path, and the repair path in the routing table:

```
Router> show ip route vrf test1 repair-paths 192.168.3.0

Routing Table: test1
Routing entry for 192.168.3.0/24
  Known via "bgp 10", distance 20, metric 0
  Tag 100, type external
  Last update from 192.168.1.1 00:49:39 ago
  Routing Descriptor Blocks:
  * 192.168.1.1, from 192.168.1.1, 00:49:39 ago, recursive-via-conn
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 100
      MPLS label: none
    [RPR]10.4.4.4 (default), from 10.5.5.5, 00:49:39 ago, recursive-via-host
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 100
      MPLS label: 29
      MPLS Flags: MPLS Required, No Global
```

Related Commands

Command	Description
show ip cache	Displays the Cisco Express Forwarding table associated with a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

show tcp ha connections

To display connection-ID-to-TCP mapping data, use the **show tcp ha connections** command in privileged EXEC mode.

show tcp ha connections

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **show tcp ha connections** command is used to display connection-ID-to-TCP mapping data.

Examples

The following is sample output from the **show tcp ha connections** command:

```
Router# show tcp ha connections

SSO enabled for 40 connections
TCB       Local Address           Foreign Address        (state)    Conn Id
71EACE60  10.0.56.1.179           10.0.56.3.58671         ESTAB      37
71EA9320  10.0.53.1.179           10.0.53.3.58659         ESTAB      34
71EA35F8  10.0.41.1.179           10.0.41.3.58650         ESTAB      22
71A21FE0  10.0.39.1.179           10.0.39.3.58641         ESTAB      20
71EAA6E0  10.0.54.1.179           10.0.54.3.58663         ESTAB      35
71EA2238  10.0.40.1.179           10.0.40.3.58646         ESTAB      21
71EABAA0  10.0.55.1.179           10.0.55.3.58667         ESTAB      36
71EAE710  10.0.28.1.179           10.0.28.3.58676         ESTAB      9
71EA2728  10.0.50.1.179           10.0.50.3.58647         ESTAB      31
720541D8  10.0.49.1.179           10.0.49.3.58642         ESTAB      30
71EAA1F0  10.0.44.1.179           10.0.44.3.58662         ESTAB      25
2180B3A8  10.0.33.1.179           10.0.33.3.58657         ESTAB      14
71EAB5B0  10.0.45.1.179           10.0.45.3.58666         ESTAB      26
21809FE8  10.0.32.1.179           10.0.32.3.58653         ESTAB      13
71EA8E30  10.0.43.1.179           10.0.43.3.58658         ESTAB      24
71EAD350  10.0.27.1.179           10.0.27.3.58672         ESTAB      8
2180A9C8  10.0.52.1.179           10.0.52.3.58655         ESTAB      33
2180A4D8  10.0.42.1.179           10.0.42.3.58654         ESTAB      23
71EABF90  10.0.26.1.179           10.0.26.3.58668         ESTAB      7
71EA3AE8  10.0.51.1.179           10.0.51.3.58651         ESTAB      32
720546C8  10.0.59.1.179           10.0.59.3.58643         ESTAB      40
```

Table 75 describes the significant fields shown in the display.

Table 75 show tcp ha connections Field Descriptions

Field	Description
SSO enabled for	Displays the number of TCP connections that support BGP Nonstop Routing (NSR) with SSO.
TCB	An internal identifier for the endpoint.
Local Address	The local IP address and port.
Foreign Address	The foreign IP address and port (at the opposite end of the connection).
(state)	TCP connection state. A connection progresses through a series of states during its lifetime. The states that follow are shown in the order in which a connection progresses through them. • LISTEN—Waiting for a connection request from any remote TCP and port. • SYNSENT—Waiting for a matching connection request after having sent a connection request. • SYNRCVD—Waiting for a confirming connection request acknowledgment after having both received and sent a connection request. • ESTAB—Indicates an open connection; data received can be delivered to the user. This is the normal state for the data transfer phase of the connection. • FINWAIT1—Waiting for a connection termination request from the remote TCP or an acknowledgment of the connection termination request previously sent.
Conn id	Identifying number of the TCP connection.

slow-peer detection

To use a policy template to specify a threshold time that dynamically determines a BGP slow peer, use the **slow-peer detection** command in policy template configuration mode. To restore the default value, use the **no** form of this command.

slow-peer detection [**threshold** *seconds*]

no slow-peer detection

Syntax Description

threshold *seconds*	(Optional) Specifies the threshold time in seconds that the timestamp of the oldest message in a peers queue can be lagging behind the current time before the BGP 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

Policy template configuration (config-router-ptmp)

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 The **neighbor slow-peer detection** command performs the same function as the **bgp slow-peer detection** command (at the address-family level), except that the **neighbor slow-peer detection** command overrides the address-family level command. When the **neighbor slow-peer detection** command is unconfigured, the system will function according to the address-family level configuration. The **slow-peer detection** command performs the same function 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 considered to be slow. The commands configured under the peer-policy template will be applied to the neighbor once it inherits the peer-policy.

```
Router(config)# router bgp 13
Router(config-router)# template peer-policy ipv4_ucast_pp1
Router(config-router-ptmp)# slow-peer detection threshold 360
```

```
Router(config-router-ptmp)# slow-peer split-update-group dynamic
```

Related Commands

Command	Description
bgp slow-peer detection	Specifies a threshold time that dynamically determines a slow peer.
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.
neighbor slow-peer split-update-group dynamic	Moves a dynamically detected slow peer to a slow update group.
slow-peer split-update-group dynamic	Moves a dynamically detected slow peer to a slow update group.

slow-peer split-update-group dynamic

To use a policy template to move a dynamically detected slow peer to a slow update group, use the **slow-peer split-update-group dynamic** command in policy template configuration mode. To disable dynamically detected slow peers from being moved to a slow update group, use the **no** form of this command.

slow-peer split-update-group dynamic [**permanent**]

no 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. It remains in the slow update group until the network administrator uses one of the **clear slow** 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

Policy template (config-router-ptmp)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

When a peer is dynamically detected to be a slow peer, the slow peer is moved to a slow update group. If a *static* slow peer update group exists, the dynamic slow peer is moved to the static slow peer update group; otherwise, a new slow peer update group is created and the peer is moved to that group.

- We recommend you configure the **permanent** keyword. If the **permanent** keyword is configured, the peer is not automatically moved to its original update group. After you resolve the root cause of the slow peer, you can use the **clear 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 policy template.

If **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. That is, detection is enabled automatically with its default threshold.

Examples

In the following example, the timestamp of the oldest message in a peers queue is compared to the current time to determine if the peer is lagging more than 360 seconds. If it is, the neighbor that sent the message is determined to be a slow peer, and is put in the slow peer update group. Because the **permanent** keyword is not configured, the slow peer will be moved back to its regular original update group after it becomes a regular peer (converges).

```
Router(config)# router bgp 13
Router(config-router)# template peer-policy ipv4_ucast_pp1
Router(config-router-ptmp)# slow-peer detection threshold 360
Router(config-router-ptmp)# slow-peer split-update-group dynamic
```

Related Commands

Command	Description
slow-peer detection	Specifies a threshold time that dynamically determines a slow peer.
show ip bgp template peer-policy	Displays locally configured peer policy templates.

slow-peer split-update-group static

To mark a BGP neighbor as a slow peer and move it to a slow update group, use the **slow-peer split-update-group static** command by using a peer policy template. To unmark the slow peer and return it to its original update group, use the **no** form of this command.

slow-peer split-update-group static

no slow-peer split-update-group static

Syntax Description

This command has no arguments or keywords.

Command Default

No peer is marked as slow and moved to a slow peer update group in a static manner using a peer policy template.

Command Modes

Peer policy template (config-router-ptmp)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

Configure a static slow peer when the peer is known to be slow (perhaps due to a slow link or low processing power).

The **neighbor slow-peer split-update-group static** command performs the same function in address-family mode.

Examples

In the following example, the neighbor is marked as a slow peer and is moved to a slow update group.

```
Router(config)# router bgp 13
Router(config-router)# template peer-policy ipv4_ucast_pp1
Router(config-router-ptmp)# slow-peer split-update-group static
```

Related Commands

Command	Description
neighbor slow-peer split-update-group static	Marks a BGP neighbor as a slow peer and moves it to a slow update group.

soo

To set the site-of-origin (SoO) value for a Border Gateway Protocol (BGP) peer policy template, use the **soo** command in policy-template configuration mode. To remove the SoO value, use the **no** form of this command.

soo *extended-community-value*

no soo

Syntax Description

extended-community-value	Specifies the VPN extended community value. The value takes one of the following formats: • A 16-bit autonomous system number, a colon, and a 32-bit number, for example: 45000:3 • A 32-bit IP address, a colon, and a 16-bit number, for example: 192.168.10.2:51 In Cisco IOS Release 12.4(24)T, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. In Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. For more details about autonomous system number formats, see the **router bgp** command.

Command Default

No SoO value is set for a BGP peer policy template.

Command Modes

Policy-template configuration (config-router-ptmp)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(24)T	Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.

Release	Modification
12.2(33)SRE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

Use this command to set the SoO value for a BGP peer policy template that a BGP neighbor can inherit. The SoO value is set for a peer policy template, and a BGP neighbor is identified under address family IPv4 VRF configuration mode to inherit the peer policy that contains the SoO value.

The SoO extended community is a BGP extended community attribute that is used to identify routes that have originated from a site so that the readvertisement of that prefix back to the source site can be prevented. The SoO extended community uniquely identifies the site from which a router has learned a route. BGP can use the SoO value associated with a route to prevent routing loops.

In releases prior to Cisco IOS Release 12.4(11)T, 12.2(33)SRB, and 12.2(33)SB, the SoO extended community attribute is configured using an inbound route map that sets the SoO value during the update process. The introduction of the **neighbor soo** and **soo** commands simplifies the SoO value configuration.

In Cisco IOS Release 12.4(24)T, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

In Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

Note If a BGP peer inherits from several peer policy templates that specify different SoO values, the SoO value in the last template applied takes precedence and is applied to the peer. However, direct configuration of the SoO value on the BGP neighbor overrides any inherited template configurations of the SoO value.

Examples

The following example shows how to create a peer policy template and configure an SoO value as part of the peer policy. Under address family IPv4 VRF, a neighbor is identified and configured to inherit the peer policy that contains the SoO value.

```
router bgp 45000
 template peer-policy SOO_POLICY
  soo 45000:3
  exit-peer-policy
 address-family ipv4 vrf SOO_VRF
  neighbor 192.168.3.2 remote-as 50000
  neighbor 192.168.3.2 activate
  neighbor 192.168.3.2 inherit peer-policy SOO_POLICY
  end
```

The following example shows how to create a peer policy template and configure an SoO value using a 4-byte autonomous system number, 1.2 in asdot format, as part of the peer policy. Under address family IPv4 VRF, a neighbor is identified and configured to inherit the peer policy that contains the SoO value. This example requires Cisco IOS Release 12.4(24)T, Cisco IOS XE Release 2.4, or a later release.

```
router bgp 1.2
 template peer-policy SOO_POLICY
  soo 1.2:3
  exit-peer-policy
 address-family ipv4 vrf SOO_VRF
  neighbor 192.168.3.2 remote-as 1.14
  neighbor 192.168.3.2 activate
  neighbor 192.168.3.2 inherit peer-policy SOO_POLICY
  end
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enters address family configuration mode to configure a routing session using standard IP Version 4 address prefixes.
neighbor soo	Sets the SoO value for a BGP neighbor or peer group.
router bgp	Configures the BGP routing process.
template peer-policy	Creates a peer policy template and enters policy-template configuration mode.

synchronization

To enable the synchronization between BGP and your Interior Gateway Protocol (IGP) system, use the **synchronization** command in address family or router configuration mode. To enable the Cisco IOS software to advertise a network route without waiting for the IGP, use the **no** form of this command.

synchronization

no synchronization

Syntax Description

This command has no arguments or keywords.

Defaults

The behavior of this command is disabled by default.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(8)T	Command default behavior changed to disabled.
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

Usually, a BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the IGP. By default, synchronization between BGP and the IGP is turned off to allow the Cisco IOS software to advertise a network route without waiting for route validation from the IGP. This feature allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems.

Use the **synchronization** command if routers in the autonomous system do not speak BGP.

Examples

The following example shows how to enable synchronization in router configuration mode. The router validates the network route in its IGP before advertising the route externally.

```
router bgp 65120
 synchronization
```

The following example shows how to enable synchronization in address family configuration mode. The router validates the network route in its IGP before advertising the route externally.

```
router bgp 65120
address-family ipv4 unicast
 synchronization
```

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 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.

table-map

To modify metric and tag values when the IP routing table is updated with BGP learned routes, use the **table-map** command in address family or router configuration mode. To disable this function, use the **no** form of the command.

table-map *map-name*

no table-map *map-name*

Syntax Description

map-name	Route map name from the **route-map** command.

Defaults

This command is disabled by default.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command adds the route map name defined by the **route-map** command to the IP routing table. This command is used to set the tag name and the route metric to implement redistribution.

You can use **match** clauses of route maps in the **table-map** command. IP access list, autonomous system paths, and next hop match clauses are supported.

Examples

In the following router configuration mode example, the Cisco IOS software is configured to automatically compute the tag value for the BGP learned routes and to update the IP routing table:

```
route-map tag
 match as path 10
 set automatic-tag
!
router bgp 100
 table-map tag
```

In the following address family configuration mode example, the Cisco IOS software is configured to automatically compute the tag value for the BGP learned routes and to update the IP routing table:

```
route-map tag
 match as path 10
 set automatic-tag
!
router bgp 100
address-family ipv4 unicast
 table-map tag
```

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 vpn4	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.
match as-path	Matches a BGP autonomous system path access list.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

template peer-policy

To create a peer policy template and enter policy-template configuration mode, use the **template peer-policy** command in router configuration mode. To remove a peer policy template, use the **no** form of this command.

template peer-policy *policy-template-name*

no template peer-policy *policy-template-name*

Syntax Description

policy-template-name	Name or tag for the peer policy template.

Defaults

Removing a peer policy template by using the **no** form of this command removes all policy configurations inside of the template.

Command Modes

Router configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Peer policy templates are used to group and apply the configuration of commands that are applied within specific address-families and NLRI configuration mode. Peer policy templates are created and configured in peer policy configuration mode. BGP policy commands that are configured for specific address-families or NLRI configuration modes are configured in a peer policy template. The following BGP policy commands are supported by peer policy templates:

- **advertisement-interval**
- **allowas-in**
- **as-override**
- **capability**
- **default-originate**
- **distribute-list**
- **dmzlink-bw**
- **exit-peer-policy**
- **filter-list**

- **inherit peer-policy**
- **maximum-prefix**
- **next-hop-self**
- **next-hop-unchanged**
- **prefix-list**
- **remove-private-as**
- **route-map**
- **route-reflector-client**
- **send-community**
- **send-label**
- **soft-reconfiguration**
- **unsuppress-map**
- **weight**

Peer policy templates are used to configure BGP policy commands that are configured for neighbors that belong to specific address-families and NLRI configuration modes. Like peer session templates, peer policy templates are configured once and then applied to many neighbors through the direct application of a peer policy template or through inheritance from peer policy templates. The configuration of peer policy templates simplifies the configuration of BGP policy commands that are applied to all neighbors within an autonomous system.

Peer policy templates support direct and indirect inheritance from up to eight peer policy templates. Inherited peer policy templates are configured with sequence numbers like route-maps. An inherited peer policy template, like a route-map, is evaluated starting with the inherit statement with the lowest sequence number and ending with the highest sequence number. However, there is a difference; a peer policy template will not fall through like a route-map. Every sequence is evaluated, and if a BGP policy command is reapplied with different value, it will overwrite any previous value from a lower sequence number.

Peer policy templates support only general policy commands. BGP policy configuration commands that are configured only for specific address families or NLRI configuration modes are configured with peer policy templates.



Note A BGP neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured to belong only to a peer group or to inherit policies from only peer templates.

Examples

The following example creates a peer policy template named CUSTOMER-A. This peer policy template is configured to inherit the configuration from the peer policy templates named PRIMARY-IN and GLOBAL.

```
Router(config-router)# template peer-policy CUSTOMER-A
Router(config-router-ptmp)# route-map SET-COMMUNITY in
Router(config-router-ptmp)# filter-list 20 in
Router(config-router-ptmp)# inherit peer-policy PRIMARY-IN 20
Router(config-router-ptmp)# inherit peer-policy GLOBAL 10
Router(config-router-ptmp)# exit-peer-policy
Router(config-router)#
```

Related Commands

Command	Description
advertisement-interval	Sets the minimum interval between the sending of BGP routing updates.
allowas-in	Configures PE routers to allow readvertisement of all prefixes containing duplicate autonomous system numbers.
as-override	Configures a PE router to override the ASN of a site with the ASN of a provider.
capability orf prefix-list	Configures outbound route filtering and advertises the capability to send and receive ORF updates to the neighbor routers.
default-originate	Originates a default route to the local router.
distribute-list	Distributes BGP neighbor information as specified in an access list.
dmzlink-bw	Advertises the bandwidth of links that are used to exit an autonomous system.
exit peer-policy	Exits policy-template configuration mode and enters router configuration mode.
filter-list	Sets up a BGP filter.
inherit peer-policy	Configures a peer policy template to inherit the configuration from another peer policy template.
maximum-prefix	Controls how many prefixes can be received from a neighbor.
neighbor inherit peer-policy	Configures a router to send a peer policy template to a neighbor so that the neighbor can inherit the configuration.
neighbor send-label	Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.
next-hop-self	Disables next-hop processing of BGP updates on the router.
next-hop-unchanged	Propagates the next- hop unchanged for iBGP paths to this router.
prefix-list	Specifies a prefix list, a CLNS filter set, or a CLNS filter expression to be used to filter BGP advertisements.
remove-private-as	Removes the private autonomous system number from outbound routing updates.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
send-community	Specifies that the BGP community attribute should be sent to the specified neighbor.
show ip bgp template peer-policy	Displays locally configured peer policy templates.
show ip bgp template peer-session	Displays locally configured peer session templates.
soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
template peer-session	Creates a peer session template and enters session-template configuration mode.
unsuppress-map	Selectively unsuppresses surpressed routes.
weight	Assigns a weight to a neighbor connection.

template peer-session

To create a peer session template and enter session-template configuration mode, use the **template peer-session** command in router configuration mode. To remove a peer session template, use the **no** form of this command.

template peer-session *session-template-name*

no template peer-session *session-template-name*

Syntax Descriptions

session-template-name	Name or tag for the peer session template.

Defaults

Removing a peer session template by using the **no** form of this command removes all session command configurations inside of the template.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Peer session templates are used to group and apply the configuration of general session commands to groups of neighbors that share common session configuration elements. General session commands that are common for neighbors that are configured in different address families can be configured within the same peer session template. Peer session templates are created and configured in peer session configuration mode. Only general session commands can be configured in a peer session template. The following general session commands are supported by peer session templates:

- **description**
- **disable-connected-check**
- **ebgp-multihop**
- **exit peer-session**
- **inherit peer-session**
- **local-as**
- **password**

- **remote-as**
- **shutdown**
- **timers**
- **translate-update**
- **update-source**
- **version**

General session commands can be configured once in a peer session template and then applied to many neighbors through the direct application of a peer session template or through indirect inheritance from a peer session template. The configuration of peer session templates simplify the configuration of general session commands that are commonly applied to all neighbors within an autonomous system.

Peer session templates support direct and indirect inheritance. A peer can be configured with only one peer session template at a time, and that peer session template can contain only one indirectly inherited peer session template. However, each inherited session template can also contain one indirectly inherited peer session template. So, only one directly applied peer session template and up to seven additional indirectly inherited peer session templates can be applied, allowing you to apply up to a maximum of eight peer session configurations to a neighbor: the configuration from the directly inherited peer session template and the configurations from up to seven indirectly inherited peer session templates. Inherited peer session templates are evaluated first, and the directly applied template will be evaluated and applied last. So, if a general session command is reapplied with a different value, the subsequent value will have priority and overwrite the previous value that was configured in the indirectly inherited template.

Peer session templates support only general session commands. BGP policy configuration commands that are configured only for specific address families or NLRI configuration modes are configured with peer policy templates.

Note A BGP neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured only to belong to a peer group or to inherit policies from peer templates.

Examples

The following example creates a peer session template named CORE1. This example inherits the configuration of the peer session template named INTERNAL-BGP.

```
Router(config-router)# template peer-session CORE1
Router(config-router-stmp)# description CORE-123
Router(config-router-stmp)# update-source loopback 1
Router(config-router-stmp)# inherit peer-session INTERNAL-BGP
Router(config-router-stmp)# exit-peer-session
Router(config-router)#
```

Related Commands

Command	Description
description	Configures a description to be displayed by the local or a peer router.
disable-connected-check	Disables connection verification for eBGP peers no more than one hop away when the eBGP peer is configured with a loopback interface.
ebgp-multihop	Accepts or initiates BGP connections to external peers residing on networks that are not directly connected.
exit peer-session	Exits session-template configuration mode and enters router configuration mode.

Command	Description
inherit peer-session	Configures a peer session template to inherit the configuration from another peer session template.
local-as	Allows the customization of the autonomous system number for eBGP peer groupings.
neighbor inherit peer-session	Configures a router to send a peer session template to a neighbor so that the neighbor can inherit the configuration.
neighbor translate-update	Upgrades a router running BGP in the NLRI format to support multiprotocol BGP.
password	Enables MD5 authentication on a TCP connection between two BGP peers.
remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
show ip bgp template peer-policy	Displays locally configured peer policy templates.
show ip bgp template peer-session	Displays locally configured peer session templates.
shutdown	Disables a neighbor or peer group.
timers bgp	Adjusts BGP network timers.
update-source	Specifies that the Cisco IOS software allow internal BGP sessions to use any operational interface for TCP connections.
version	Configures the Cisco IOS software to accept only a particular BGP version.

timers bgp

To adjust BGP network timers, use the **timers bgp** command in router configuration mode. To reset the BGP timing defaults, use the **no** form of this command.

timers bgp *keepalive holdtime* [*min-holdtime*]

no timers bgp

Syntax Description

keepalive	Frequency (in seconds) with which the Cisco IOS software sends *keepalive* messages to its peer. The default is 60 seconds. The range is from 0 to 65535.
holdtime	Interval (in seconds) after not receiving a *keepalive* message that the software declares a peer dead. The default is 180 seconds. The range is from 0 to 65535.
min-holdtime	(Optional) Interval (in seconds) specifying the minimum acceptable hold-time from a BGP neighbor. The minimum acceptable hold-time must be less than, or equal to, the interval specified in the *holdtime* argument. The range is from 0 to 65535.

Defaults

keepalive: 60 seconds
holdtime: 180 seconds

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(26)S	The *min-holdtime* argument was added.
12.3(7)T	The *min-holdtime* argument was added.
12.2(22)S	The *min-holdtime* argument was added.
12.2(27)SBC	The *min-holdtime* argument was added and this command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	The *min-holdtime* argument was added and this command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	The *min-holdtime* argument was added and this command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

When configuring the *holdtime* argument for a value of less than twenty seconds, the following warning is displayed:

```
% Warning: A hold time of less than 20 seconds increases the chances of peer flapping
```

If the minimum acceptable hold-time interval is greater than the specified hold-time, a notification is displayed:

```
% Minimum acceptable hold time should be less than or equal to the configured hold time
```

Note When the minimum acceptable hold-time is configured on a BGP router, a remote BGP peer session is established only if the remote peer is advertising a hold-time that is equal to, or greater than, the minimum acceptable hold-time interval. If the minimum acceptable hold-time interval is greater than the configured hold-time, the next time the remote session tries to establish, it will fail and the local router will send a notification stating "unacceptable hold time."

Examples

The following example changes the keepalive timer to 70 seconds, the hold-time timer to 130 seconds, and the minimum acceptable hold-time interval to 100 seconds:

```
router bgp 45000
 timers bgp 70 130 100
```

Related Commands

Command	Description
clear ip bgp peer-group	Removes all the members of a BGP peer group.
router bgp	Configures the BGP routing process.
show ip bgp	Displays entries in the BGP routing table.