



R3.3 Beta Draft—Cisco Confidential Information



Cisco IOS XR Routing Command Reference

Cisco IOS XR Software Release 3.3

Corporate 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: 408 526-4100

Text Part Number: OL-8508-01



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.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0502R)

Cisco IOS XR Routing Command Reference
Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Preface

Beta Draft Cisco Confidential Information

This document describes the commands used to display and configure routing on Cisco IOS XR software.

For routing configuration information and examples, refer to the *Cisco IOS XR Routing Configuration Guide*.

The preface for *Cisco IOS XR Routing Command Reference* contains the following sections:

- [Obtaining Documentation, page iii](#)
- [Documentation Feedback, page iv](#)
- [Cisco Product Security Overview, page v](#)
- [Obtaining Technical Assistance, page vi](#)
- [Obtaining Additional Publications and Information, page vii](#)

Document Revision History

The Document Revision History table below records technical changes to this document. The table shows the document revision number for the change, the date of the change, and a brief summary of the change.

Revision	Date	Change Summary
OL-8508-01	December 2005	This is the initial release.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

R3.3 Beta Draft—Cisco Confidential Information

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

R3.3 Beta Draft—Cisco Confidential Information

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

R3.3 Beta Draft—Cisco Confidential Information

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

R3.3 Beta Draft—Cisco Confidential Information

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

R3.3 Beta Draft—Cisco Confidential Information

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

BGP Commands on Cisco IOS XR Software

Beta Draft Cisco Confidential Information

This chapter describes the commands used to configure and monitor Border Gateway Protocol (BGP) for IP Version 4 (IPv4), IP Version 6 (IPv6), and Virtual Private Network Version 4 (VPNv4) routing sessions.

For detailed information about BGP concepts, configuration tasks, and examples, see the *Implementing BGP on Cisco IOS XR Software* configuration guide.

R3.3 Beta Draft—Cisco Confidential Information

address-family (BGP)

To enter various address family configuration modes while configuring Border Gateway Protocol (BGP), use the **address-family** command in an appropriate configuration mode. To disable support for an address family, use the **no** form of this command.

address-family { **ipv4 unicast** | **ipv4 multicast** | **ipv6 unicast** | **ipv6 multicast** | **vpnv4 unicast** }

no address-family { **ipv4 unicast** | **ipv4 multicast** | **ipv6 unicast** | **ipv6 multicast** | **vpnv4 unicast** }

Syntax Description

ipv4 unicast	Specifies IP Version 4 (IPv4) unicast address prefixes.
ipv4 multicast	Specifies IPv4 multicast address prefixes.
ipv6 unicast	Specifies IP Version 6 (IPv6) unicast address prefixes.
ipv6 multicast	Specifies IPv6 multicast address prefixes.
vpnv4 unicast	Specifies VPN Version 4 (VPNv4) unicast address prefixes.

Defaults

An address family must be explicitly configured in the router configuration mode for the address family to be active in BGP. Similarly, an address family must be configured under the neighbor for the BGP session to be established for that address family. An address family must be configured in router configuration mode before it can be configured under a neighbor.

Command Modes

Router configuration
 Neighbor configuration (IPv4, IPv6 and VPNv4 address families)
 Neighbor group configuration
 VRF configuration
 VRF neighbor configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	The vpnv4 unicast keywords were added. This command was supported in VRF and VRF neighbor configuration modes.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **address-family** command to enter various address family configuration modes while configuring BGP routing sessions. When you enter the **address-family** command from router configuration mode, you enable the address family and enter global address family configuration mode.

When you enter the **address-family** command from neighbor configuration mode, you activate the address family on the neighbor and enter neighbor address family configuration mode.

R3.3 Beta Draft—Cisco Confidential Information

For IPv4 neighbors, the default address family is IPv4 unicast.



Note

It is not necessary to have an address family configured in router configuration mode for either an IPv4 or IPv6 neighbor to be configured. However, to be able to configure an address family under a neighbor, the same address family must be configured in router configuration mode. It is not possible to bring up a session for a neighbor under a specific address family unless the address family is configured for the neighbor.

Task ID	Task ID	Operations
	bgp	read, write

Examples

The following example shows how to place the router in global address family configuration mode for the IPv4 address family:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router bgp 100
RP/0/RP0/CPU0:router(config-bgp)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)#
```

The following example shows how to activate IPv4 multicast for neighbor 10.0.0.1 and place the router in neighbor address family configuration mode for the IPv4 multicast address family:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# address-family ipv4 multicast
RP/0/RP0/CPU0:router(config-bgp-af)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.0.0.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 multicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)#
```

R3.3 Beta Draft—Cisco Confidential Information

advertisement-interval

To set the minimum interval between the sending of Border Gateway Protocol (BGP) routing updates, use the **advertisement-interval** command in an appropriate configuration mode. To remove the **advertisement-interval** command from the configuration file and restore the system to its default interval values, use the **no** form of this command.

advertisement-interval *seconds*

no advertisement-interval

Syntax Description

<i>seconds</i>	Minimum interval between sending BGP routing updates (in seconds). Range is 0 to 600.

Defaults

Default minimum interval is 30 seconds for external peers and 5 seconds for internal peers.

Command Modes

Neighbor configuration
 Neighbor group configuration
 Session group configuration
 VRF neighbor configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF neighbor configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If this command configures a neighbor group or session group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to set the minimum time between sending BGP routing updates to 10 seconds:

```
RP/0/RP0/CPU0:router(config)# router bgp 5
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.1.1.1
```

R3.3 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 100
RP/0/RP0/CPU0:router(config-bgp-nbr)# advertisement-interval 10
```

Related Commands

Command	Description
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
session-group	Creates a session group and enters session group configuration mode.

R3.3 Beta Draft—Cisco Confidential Information

af-group

To create an address family group for Border Gateway Protocol (BGP) neighbors and enter address family group configuration mode, use the **af-group** command in router configuration mode. To remove an address family group, use the **no** form of this command.

af-group *af-group-name* **address-family** { **ipv4 unicast** | **ipv4 multicast** | **ipv6 unicast** | **ipv6 multicast** | **vpn4 unicast** }

no af-group *af-group-name* **address-family** { **ipv4 unicast** | **ipv4 multicast** | **ipv6 unicast** | **ipv6 multicast** | **vpn4 unicast** }

Syntax Description

<i>af-group-name</i>	Address family group name.
address-family	Enters address family configuration mode.
ipv4 unicast	Specifies IP Version 4 (IPv4) unicast address prefixes.
ipv4 multicast	Specifies IPv4 multicast address prefixes.
ipv6 unicast	Specifies IP Version 6 (IPv6) unicast address prefixes.
ipv6 multicast	Specifies IPv6 multicast address prefixes.
vpn4 unicast	Specifies VPN Version 4 (VPNv4) unicast address prefixes.

Defaults

No BGP address family group is configured.

Command Modes

Router configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	The vpn4 unicast keywords were added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **af-group** command to group address family-specific neighbor commands within an IPv4 or IPv6 address family. Neighbors that have address family configuration are able to use the address family group. Further, neighbors inherit the configuration parameters of the entire address family group. This feature replaces part of the functionality of peer groups found in previous Cisco IOS XR software releases.

You cannot define two address family groups with the same name in different address families.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	bgp	read, write

Examples

The following example shows how to create address family group group1 and enter address family group configuration mode for IPv4 unicast. Group1 contains the next-hop-self feature, which is inherited by neighbors that want to use address family group1.

```
RP/0/RP0/CPU0:router(config)# router bgp 100
RP/0/RP0/CPU0:router(config-bgp)# af-group group1 address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-afgrp)# next-hop-self
```

Related Commands

Command	Description
neighbor (BGP)	Enters neighbor configuration mode for configuring BGP routing sessions.
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
session-group	Creates a session group and enters session group configuration mode.
use	Inherits configuration from a neighbor group, session group, or address family group.

R3.3 Beta Draft—Cisco Confidential Information

aggregate-address

To create an aggregate entry in a Border Gateway Protocol (BGP) routing table, use the **aggregate-address** command in an appropriate configuration mode. To remove the **aggregate-address** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

aggregate-address *address/mask-length* [**as-set**] [**as-confed-set**] [**summary-only**] [**route-policy** *route-policy-name*]

no aggregate-address *address/mask-length*

Syntax Description

<i>address</i>	Aggregate address.
<i>/mask-length</i>	Aggregate address mask length.
as-set	(Optional) Generates autonomous system set path information and community information from contributing paths.
as-confed-set	(Optional) Generates autonomous system confederation set path information from contributing paths.
summary-only	(Optional) Filters all more-specific routes from updates.
route-policy <i>route-policy-name</i>	(Optional) Specifies the name of a route policy used to set the attributes of the aggregate route.

Defaults

When you do not specify this command, no aggregate entry is created in the BGP routing table.

Command Modes

IPv4 address family configuration
IPv6 address family configuration
VRF IPv4 address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The policy keyword was changed to route-policy .
Release 3.3	This command was supported in VRF IPv4 address family configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You can implement aggregate routing in BGP either by redistributing an aggregate route into BGP using the **network** command or the **aggregate-address** command.

R3.3 Beta Draft—Cisco Confidential Information

Use the **aggregate-address** command without optional arguments to create an aggregate entry in the BGP routing table if any more-specific BGP routes are available that fall in the specified range. The aggregate route is advertised as coming from your autonomous system and has 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.)

Use of the **as-set** keyword creates an aggregate entry using the same rules that the command follows without this keyword. However, the advertised path for this route is an AS_SET, a set of all autonomous systems 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.

Use the **as-confed-set** keyword to create an AS_CONFED_SET in the autonomous system path of the aggregate from any confederation segments in the paths being summarized. This keyword takes effect only if the **as-set** keyword is also specified.

Use of the **summary-only** keyword creates an aggregate entry (for example, 10.0.0.0/8) but suppresses advertisements of more-specific routes to all neighbors. If you want to suppress only advertisements to certain neighbors, use the **route-policy (BGP)** command in neighbor address family configuration mode with caution. If a more-specific route leaks out, all BGP speakers (the local router) prefer that route over the less-specific aggregate you generate (using longest-match routing).

Use the **route-policy** keyword to specify a routing policy for the aggregate entry. The **route-policy** keyword is used to select which more-specific information to base the aggregate entry on and which more-specific information to suppress. You can also use the keyword to modify the attributes of the aggregate entry.

Task ID	Task ID	Operations
	bgp	read, write

Examples The following example shows how to create an aggregate address. The path advertised for this route is an autonomous system set consisting of all elements contained in all paths that are being summarized.

```
RP/0/RP0/CPU0:router(config)# router bgp 100
RP/0/RP0/CPU0:router(config-bgp)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-af)# aggregate-address 10.0.0.0/8 as-set
```

Related Commands	Command	Description
	network (BGP)	Specifies the list of networks for the BGP routing process.
	route-policy (BGP)	Applies a routing policy to updates advertised to or received from a BGP neighbor
	route-policy (RPL)	Defines a route policy and enters route-policy configuration mode.
	update-source	Advertises routes previously suppressed by the aggregate-address command.

R3.3 Beta Draft—Cisco Confidential Information

allowas-in

To allow an AS path with the provider edge (PE) autonomous system number (ASN) a specified number of times, use the **allowas-in** command in an appropriate configuration mode. To restore the system to its default condition, use the **no** form of this command.

allowas-in [*as-occurrence-number*]

no allowas-in [*as-occurrence-number*]

Syntax Description

as-occurrence-number (Optional) Number of times a PE ASN is allowed. Range is 1 to 10.

Defaults

No default behavior or values

Command Modes

Address family group configuration
Neighbor address family configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Hub and spoke VPN networks require looping back of routing information to the hub PE through the hub customer edge (CE). See the *Cisco IOS XR Routing Configuration Guide* for information on hub and spoke VPN networks. This looping back, in addition to the presence of the PE ASN, causes the looped-back information to be dropped by the hub PE.

The **allowas-in** command prevents the looped-back information from being dropped by replacing the neighbor autonomous system number (ASN) with the PE ASN in the AS path. This allows the VPN customer to see a specified number of occurrences of the PE ASN in the AS path.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to allow five occurrences of the PE ASN:

```
RP/0/RP0/CPU0:router(config)# router bgp 6
RP/0/RP0/CPU0:router(config-bgp)# af-group group_1 address-family vpnv4 unicast
RP/0/RP0/CPU0:router(config-bgp-afgrp)# allowas-in 5
```

R3.3 Beta Draft—Cisco Confidential Information

bgp as-path-loopcheck

To enable an autonomous system path for loop checking internal Border Gateway Protocol (iBGP) peers, use the **bgp as-path-loopcheck** command in an appropriate configuration mode. To restore the system to its default condition, use the **no** form of this command.

bgp as-path-loopcheck

no bgp as-path-loopcheck

Syntax Description This command has no arguments or keywords.

Defaults When you do not specify this command, loop checking is performed only for external peers.

Command Modes Router configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	bgp	read, write

Examples The following example shows how to configure an autonomous system path for loop checking iBGP peers:

```
RP/0/RP0/CPU0:router(config)# router bgp 6
RP/0/RP0/CPU0:router(config-bgp)# bgp as-path-loopcheck
```

R3.3 Beta Draft—Cisco Confidential Information

bgp attribute-download

To enable Border Gateway Protocol (BGP) attribute download, use the **bgp attribute-download** command in an appropriate configuration mode. To disable BGP attribute download, use the **no** form of this command.

bgp attribute-download

no bgp attribute-download

Syntax Description This command has no arguments or keywords.

Defaults BGP attribute download is not enabled.

Command Modes IPv4 unicast address family configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When BGP attribute download is enabled using the **bgp attribute-download** command, BGP reinstalls all routes whose attributes are not currently in the RIB. Likewise, if the user disables BGP attribute download using the **no** form of the command, BGP reinstalls previously installed routes with a null key, and removes the attributes from the RIB.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to enable BGP attribute download on BGP router 50:

```
RP/0/RP0/CPU0:router(config)# router bgp 50
RP/0/RP0/CPU0:router(config-bgp)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-af)# bgp attribute-download
```

R3.3 Beta Draft—Cisco Confidential Information

bgp auto-policy-soft-reset disable

To disable an automatic reset of Border Gateway Protocol (BGP) peers when their configured route policy is modified, use the **bgp auto-policy-soft-reset disable** command in an appropriate configuration mode. To re-enable automatic soft reset of BGP peers, use the **no** form of this command.

bgp auto-policy-soft-reset disable

no bgp auto-policy-soft-reset disable

Syntax Description This command has no arguments or keywords.

Defaults Automatic soft reset of peers is enabled.

Command Modes Router configuration
VRF configuration

Command History	Release	Modification
	Release 2.0	This command was first introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router. The disable keyword was changed from optional to mandatory.
	Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

If the inbound policy changes, it is not always possible to perform a soft reset. This is the case if the neighbor does not support route refresh and soft-reconfiguration inbound is not configured for the neighbor. In such instances, a message is logged in the system log indicating that a manual hard reset is needed.

Task ID	Task ID	Operations
	bgp	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to disable an automatic soft reset of BGP peers when their configured route policy is modified:

```
RP/0/RP0/CPU0:router(config)# router bgp 6  
RP/0/RP0/CPU0:router(config-bgp)# bgp auto-policy-soft-reset disable
```

R3.3 Beta Draft—Cisco Confidential Information

bgp bestpath as-path ignore

To ignore the autonomous system path length when calculating preferred paths, use the **bgp bestpath as-path ignore** command in an appropriate configuration mode. To return the software to the default state in which it considers the autonomous system path length when calculating preferred paths, 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.

Defaults

The autonomous system path length is used (not ignored) when a best path is selected.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **bgp bestpath as-path ignore** command to ignore the length of autonomous system paths when the software selects a preferred path. When the best path is selected, if this command is specified, all steps are performed as usual except comparison of the autonomous path length between candidate paths.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to configure the software to ignore the autonomous system length when performing best path selection:

```
RP/0/RP0/CPU0:router(config)# router bgp 65000
RP/0/RP0/CPU0:router(config-bgp)# bgp bestpath as-path ignore
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	bgp bestpath compare-routerid	Compares identical routes received from eBGP peers during the best path selection process and selects the route with the lowest router ID.
	bgp bestpath med always	Allows the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems.
	bgp bestpath med confed	Enables MED comparison among paths learned from confederation peers.
	bgp bestpath med missing-as-worst	Enables the software to consider a missing MED attribute in a path as having a value of infinity.

R3.3 Beta Draft—Cisco Confidential Information

bgp bestpath compare-routerid

To compare identical routes received from external BGP (eBGP) peers during the best path selection process and select the route with the lowest router ID, use the **bgp bestpath compare-routerid** command in an appropriate configuration mode. To disable comparing identical routes received from eBGP peers during best path selection, use the **no** form of this command.

bgp bestpath compare-routerid

no bgp bestpath compare-routerid

Syntax Description

This command has no arguments or keywords.

Defaults

The software does not select a new best path if it is the same as the current best path (according to the BGP selection algorithm) except for the router ID.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **bgp bestpath compare-routerid** command to affect how the software selects the best path, in the case where there are two paths of equal cost according to the BGP selection algorithm. This command is used to force the software to select the path with the lower router ID as the best path. If this command is not used, the software continues to use whichever path is currently the best path, regardless of which has the lower router ID.

Task ID

Task ID	Operations
bgp	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to configure the BGP speaker in autonomous system 500 to compare the router IDs of similar paths:

```
RP/0/RP0/CPU0:router(config)# router bgp 500  
RP/0/RP0/CPU0:router(config-bgp)# bgp bestpath compare-routerid
```

Related Commands

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

R3.3 Beta Draft—Cisco Confidential Information

bgp bestpath med always

To allow the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems, use the **bgp bestpath med always** command in an appropriate configuration mode. To disable considering the MED attribute in comparing paths, use the **no** form of this command.

bgp bestpath med always

no bgp bestpath med always

Syntax Description

This command has no arguments or keywords.

Defaults

The software does not compare MEDs for paths between neighbors in different autonomous systems.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The MED is one of the parameters that is considered by the software when selecting the best path among many alternative paths. The software chooses the path with the lowest MED.

By default, during the best path selection process, the software makes a MED comparison only among paths from the same autonomous system. This command changes the default behavior of the software by allowing comparison of MEDs, among paths regardless of the autonomous system from which the paths are received.

Task ID

Task ID	Operations
bgp	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to configure the Border Gateway Protocol (BGP) speaker in autonomous system 100 to compare MEDs among alternative paths, regardless of the autonomous system from which the paths are received:

```
RP/0/RP0/CPU0:router(config)# router bgp 100  
RP/0/RP0/CPU0:router(config-bgp)# bgp bestpath med always
```

Related Commands

Command	Description
bgp bestpath med confed	Enables MED comparison among paths learned from confederation peers.
bgp bestpath med missing-as-worst	Specifies that the software consider a missing MED attribute in a path as having a value of infinity, making the path without a MED value the least desirable path.
show bgp	Displays entries in the BGP routing table.

R3.3 Beta Draft—Cisco Confidential Information

bgp bestpath med confed

To enable Multi Exit Discriminator (MED) comparison among paths learned from confederation peers, use the **bgp bestpath med confed** command in an appropriate configuration mode. To disable the software from considering the MED attribute in comparing paths, use the **no** form of this command.

bgp bestpath med confed

no bgp bestpath med confed

Syntax Description

This command has no arguments or keywords.

Defaults

The software does not compare the MED of paths containing only confederation segments, or paths containing confederation segments followed by an AS_SET, with the MED of any other paths.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

By default, the MED of the following paths is not compared with the MED of any other path:

- Paths with an empty autonomous system path
- Paths beginning with an AS_SET
- Paths containing only confederation segments
- Paths containing confederation segments followed by an AS_SET

Use the **bgp bestpath med confed** command to affect how the following types of paths are treated in the BGP best path algorithm:

- Paths containing only confederation segments
- Paths containing confederation segments followed by an AS_SET

The MED for paths that start with an AS_SEQUENCE or that start with confederation segments followed by an AS_SEQUENCE only is compared with the MED of other paths that share the same first autonomous system number in the autonomous system sequence (the neighbor autonomous system number). This behavior is not affected by the **bgp bestpath med confed** command.

R3.3 Beta Draft—Cisco Confidential Information

As an example, suppose that autonomous systems 65000, 65001, 65002, and 65004 are part of a confederation, but autonomous system 1 is not. Suppose that for a particular route, the following paths exist:

- Path 1: 65000 65004, med = 2, IGP metric = 20
- Path 2: 65001 65004, med = 3, IGP metric = 10
- Path 3: 65002 1, med = 1, IGP metric = 30

If the **bgp bestpath med confed** command is enabled, the software selects path 1 as the best path because it:

- Has a lower MED than path 2
- Has a lower IGP metric than path 3

The MED is not compared with path 3 because it has an external autonomous system number (that is, an AS_SEQUENCE) in the path. If the **bgp bestpath med confed** command is not enabled, then MED is not compared between any of these paths. Consequently, the software selects path 2 as the best path because it has the lowest IGP metric.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following command shows how to enable Border Gateway Protocol (BGP) software to compare MED values for paths learned from confederation peers:

```
RP/0/RP0/CPU0:router(config)# router bgp 210
RP/0/RP0/CPU0:router(config-bgp)# bgp bestpath med confed
```

Related Commands

Command	Description
bgp bestpath med always	Enables MED comparison among paths from neighbors in different autonomous systems.
bgp bestpath med missing-as-worst	Specifies that the software consider a missing MED attribute in a path as having a value of infinity, making the path without a MED value the least desirable path.
show bgp	Displays entries in the BGP routing table.

R3.3 Beta Draft – Cisco Confidential Information

bgp bestpath med missing-as-worst

To have the software consider a missing Multi Exit Discriminator (MED) attribute in a path as having a value of infinity, making the path without a MED value the least desirable path, use the **bgp bestpath med missing-as-worst** command in an appropriate configuration mode. To disable considering the MED attribute in comparing paths, 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

The software assigns a value of 0 to the missing MED, causing the path with the missing MED attribute to be considered as the best possible MED.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to direct the Border Gateway Protocol (BGP) software to consider a missing MED attribute in a path as having a value of infinity, making this path the least desirable path:

```
RP/0/RP0/CPU0:router(config)# router bgp 210  
RP/0/RP0/CPU0:router(config-bgp)# bgp bestpath med missing-as-worst
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	bgp bestpath med always	Enables MED comparison among paths from neighbors in different autonomous systems.
	bgp bestpath med confed	Enables MED comparison among paths learned from confederation peers.
	show bgp	Displays entries in the BGP routing table.

R3.3 Beta Draft—Cisco Confidential Information

bgp cluster-id

To configure the cluster ID if the Border Gateway Protocol (BGP) cluster has more than one route reflector, use the **bgp cluster-id** command in an appropriate configuration mode. To remove the cluster ID, use the **no** form of this command.

bgp cluster-id *cluster-id*

no bgp cluster-id

Syntax Description

<i>cluster-id</i>	Cluster ID of this router acting as a route reflector; maximum of 4 bytes. Cluster ID can be entered either as an IP address or value. Range is 1 to 429496729.

Defaults

A cluster ID is not configured.

Command Modes

Router configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Together, a route reflector and its clients form a *cluster*. A cluster of clients usually has a single route reflector. In such instances, the cluster is identified by the software as the router ID of the route reflector. To increase redundancy and avoid a single point of failure in the network, a cluster might have more than one route reflector. If it does, all route reflectors in the cluster must be configured with the same 4-byte cluster ID so that a route reflector can recognize updates from route reflectors in the same cluster.

If the cluster has more than one route reflector, use the **bgp cluster-id** command to configure the cluster ID.

Task ID

Task ID	Operations
bgp	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to configure the local router as one of the route reflectors serving the cluster. It is configured with the cluster ID to identify the cluster.

```
RP/0/RP0/CPU0:router(config)# router bgp 65534
RP/0/RP0/CPU0:router(config-bgp)# bgp cluster-id 192.168.70.1
RP/0/RP0/CPU0:router(config-bgp)# neighbor 192.168.70.24
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 65534
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# route-reflector-client
```

Related Commands

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

R3.3 Beta Draft—Cisco Confidential Information

bgp confederation identifier

To specify a Border Gateway Protocol (BGP) confederation identifier, use the **bgp confederation identifier** command in an appropriate configuration mode. To remove the confederation identifier, use the **no** form of this command.

bgp confederation identifier *autonomous-system-number*

no bgp confederation identifier

Syntax Description

<i>autonomous-system-number</i>	Autonomous system number that internally includes multiple autonomous systems.

Defaults

No confederation identifier is configured.

Command Modes

Router configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

One way to reduce the internal BGP (iBGP) mesh is to divide an autonomous system into multiple autonomous systems and group them into a single confederation. Each autonomous system is fully meshed within itself, and has a few connections to another autonomous system in the same confederation. Although the peers in different autonomous systems have external BGP (eBGP) sessions, they exchange routing information as if they are iBGP peers. Specifically, the confederation maintains the next hop and local preference information, and that allows you to retain a single Interior Gateway Protocol (IGP) for all autonomous systems. To the outside world, the confederation looks like a single autonomous system.

Use the **bgp confederation identifier** command to specify the autonomous system number for the confederation. This autonomous system number is used when BGP sessions are established with external peers in autonomous systems that are not part of the confederation.

Task ID

Task ID	Operations
bgp	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to divide the autonomous system into autonomous systems 4001, 4002, 4003, 4004, 4005, 4006, and 4007 with the confederation identifier 5. Neighbor 10.2.3.4 is a router inside the confederation. Neighbor 172.20.16.6 is outside the routing domain confederation. To the outside world, there appears to be a single autonomous system with the number 5.

```
RP/0/RP0/CPU0:router(config)# router bgp 4001
RP/0/RP0/CPU0:router(config-bgp)# bgp confederation identifier 5
RP/0/RP0/CPU0:router(config-bgp)# bgp confederation peers 4002
RP/0/RP0/CPU0:router(config-bgp)# bgp confederation peers 4003
RP/0/RP0/CPU0:router(config-bgp)# bgp confederation peers 4004
RP/0/RP0/CPU0:router(config-bgp)# bgp confederation peers 4005
RP/0/RP0/CPU0:router(config-bgp)# bgp confederation peers 4006
RP/0/RP0/CPU0:router(config-bgp)# bgp confederation peers 4007
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.2.3.4
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 4002
RP/0/RP0/CPU0:router(config-bgp-nbr)# exit
RP/0/RP0/CPU0:router(config-bgp)# exit
RP/0/RP0/CPU0:router(config-bgp-nbr)# neighbor 172.20.16.6
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 4009
```

Related Commands

Command	Description
bgp confederation peers	Configures the autonomous systems that belong to the confederation.

R3.3 Beta Draft—Cisco Confidential Information

bgp confederation peers

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

bgp confederation peers *autonomous-system-number*

no bgp confederation peers *autonomous-system-number*

Syntax Description

<i>autonomous-system-number</i>	Autonomous system numbers for Border Gateway Protocol (BGP) peers that belong to the confederation. Enter one autonomous system number for each command line.

Defaults

No BGP peers are identified as belonging to the confederation.

Command Modes

Router configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows that autonomous systems 1090, 1091, 1092, and 1093 belong to a single confederation:

```
RP/0/RP0/CPU0:router(config)# router bgp 1090
RP/0/RP0/CPU0:router(config-bgp)# bgp confederation peers 1091
RP/0/RP0/CPU0:router(config-bgp)# bgp confederation peers 1092
RP/0/RP0/CPU0:router(config-bgp)# bgp confederation peers 1093
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	bgp confederation identifier	Specifies a BGP confederation identifier.

R3.3 Beta Draft—Cisco Confidential Information

bgp dampening

To enable Border Gateway Protocol (BGP) route dampening or change various BGP route dampening factors, use the **bgp dampening** command in an appropriate configuration mode. To disable route dampening and reset default values, use the **no** form of this command.

bgp dampening [*half-life* [*reuse suppress max-suppress-time*] | **route-policy** *route-policy-name*]

no bgp dampening

Syntax Description	
<i>half-life</i>	(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). Penalty reduction happens every 5 seconds. Range of the half-life period is from 1 to 45 minutes.
<i>reuse</i>	(Optional) Value for route reuse if the flapping route penalty decreases and falls below the reuse value. When this happens, the route is unsuppressed. The process of unsuppressing routes occurs at 10-second increments. Range is 1 to 20000.
<i>suppress</i>	(Optional) Maximum penalty value. Suppress a route when its penalty exceeds the value specified. When this happens, the route is suppressed. Range is 1 to 20000.
<i>max-suppress-time</i>	(Optional) Maximum time (in minutes) a route can be suppressed. Range is 1 to 20000. If the <i>half-life</i> value is allowed to default, the maximum suppress time defaults to 60 minutes.
route-policy <i>route-policy-name</i>	(Optional) Specifies the route policy to use to set dampening parameters.

Defaults

Route dampening is disabled.
half-life: 15 minutes
reuse: 750
suppress: 2000
max-suppress-time: four times *half-life* value

Command Modes

IPv4 address family configuration
 IPv6 address family configuration
 VPNv4 address family configuration
 VRF IPv4 address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Release	Modification
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The policy keyword was changed to route-policy .
Release 3.3	This command was supported in the following configuration modes: • VPNv4 address family • VRF IPv4 address family

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **bgp dampening** command without arguments to enable BGP route dampening with the default parameters. The parameters can be changed by setting them on the command line or specifying them with a routing policy.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to set the *half-life* value to 30 minutes, the *reuse* value to 1500, the *suppress* value to 10000, and the *max-suppress-time* to 120 minutes:

```
RP/0/RP0/CPU0:router(config)# router bgp 50
RP/0/RP0/CPU0:router(config-bgp)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-af)# bgp dampening 30 1500 10000 120
```

Related Commands

Command	Description
clear bgp dampening	Clears BGP route dampening information and unsuppresses the suppressed routes.
clear bgp flap-statistics	Clears BGP flap statistics.
route-policy (RPL)	Defines a route policy and enters route-policy configuration mode.
show bgp dampened-paths	Displays BGP dampened routes.
show bgp flap-statistics	Displays BGP flap statistics.
show bgp neighbors	Displays information about BGP connections to neighbors.

R3.3 Beta Draft—Cisco Confidential Information

bgp default local-preference

To change the default local preference value, use the **bgp default local-preference** command in an appropriate configuration mode. To reset the local preference value to the default of 100, use the **no** form of this command.

bgp default local-preference *value*

no bgp default local-preference

Syntax Description

<i>value</i>	Local preference value. Range is 0 to 429496725. Higher values are preferable.

Defaults

Enabled with a value of 100.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Generally, the default value of 100 allows you to easily define a particular path as less preferable than paths with no local preference attribute. The preference is sent to all networking devices in the local autonomous system.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to raise the default local preference value from the default of 100 to 200:

```
RP/0/RP0/CPU0:router(config)# router bgp 200
RP/0/RP0/CPU0:router(config-bgp)# bgp default local-preference 200
```

R3.3 Beta Draft—Cisco Confidential Information

bgp enforce-first-as disable

To disable the software from enforcing the first autonomous system path (known as the AS path) of a route received from an external Border Gateway Protocol (eBGP) peer to be the same as the configured remote autonomous system, use the **bgp enforce-first-as disable** command in an appropriate configuration mode. To re-enable enforcing the first AS path of a received route from an eBGP peer to be the same as the remote autonomous system, use the **no** form of this command.

bgp enforce-first-as disable

no bgp enforce-first-as disable

Syntax Description This command has no arguments or keywords.

Defaults By default, the software requires the first autonomous system (in the AS path) of a route received from an eBGP peer to be the same as the remote autonomous system configured.

Command Modes Router configuration
VRF configuration

Command History	Release	Modification
	Release 2.0	This command was first introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router. The disable keyword was changed from optional to mandatory.
	Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

By default, the software ignores any update received from an eBGP neighbor that does not have the autonomous system configured for that neighbor at the beginning of the AS path. When configured, the command applies to all eBGP peers of the router.

Task ID	Task ID	Operations
	bgp	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows a configuration in which incoming updates from eBGP neighbors are not checked to ensure the first AS number in the AS path is the same as the configured AS number for the neighbor:

```
RP/0/RP0/CPU0:router(config)# router bgp 100  
RP/0/RP0/CPU0:router(config-bgp)# bgp enforce-first-as disable
```

Related Commands

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

R3.3 Beta Draft—Cisco Confidential Information

bgp fast-external-fallover disable

To disable immediately resetting the Border Gateway Protocol (BGP) sessions of any directly adjacent external peers if the link used to reach them goes down, use the **bgp fast-external-fallover disable** command in an appropriate configuration mode. To disable this function and perform an immediate reset of BGP sessions when a link between peers is lost, use the **no** form of this command.

bgp fast-external-fallover disable

no bgp fast-external-fallover disable

Syntax Description	disable	Disables BGP fast external failover.

Defaults	BGP sessions of any directly adjacent external peers are immediately reset if the link used to reach them goes down.

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was first introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was first supported on the Cisco XR 12000 Series Router. The disable keyword was changed from optional to mandatory.
	Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. By default, BGP sessions of any directly adjacent external peers are immediately reset, which allows the network to recover faster when links go down between BGP peers.

Task ID	Task ID	Operations
	bgp	read, write

Examples The following example shows how to disable the automatic resetting of BGP sessions:

```
RP/0/RP0/CPU0:router(config)# router bgp 109
RP/0/RP0/CPU0:router(config-bgp)# bgp fast-external-fallover disable
```

R3.3 Beta Draft—Cisco Confidential Information

bgp graceful-restart

To enable graceful restart support, use the **bgp graceful-restart** command in an appropriate configuration mode. To disable this function, use the **no** form of this command.

bgp graceful-restart

no bgp graceful-restart

Syntax Description

This command has no arguments or keywords.

Defaults

Graceful restart support is not enabled.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **bgp graceful-restart** command to enable graceful restart functionality on the router, and also to advertise graceful restart to neighboring routers.



Note

The **bgp graceful-restart** command with no options must be used to enable graceful restart before using the **bgp graceful-restart purge-time**, **bgp graceful-restart restart-time**, **bgp graceful-restart stalepath-time**, or **bgp graceful-restart graceful-reset** commands.

When graceful restart is enabled, the BGP graceful restart capability is negotiated with neighbors in the BGP OPEN message when the session is established. If the neighbor also advertises support for graceful restart, then graceful restart is activated for that neighbor session. If the neighbor does not advertise support for graceful restart, then graceful restart is not activated for that neighbor session even though it is enabled locally.

If you enter the **bgp graceful-restart** command after some BGP sessions are established, you must restart those sessions before graceful restart takes effect. Use the **clear bgp** command to restart sessions.

R3.3 Beta Draft—Cisco Confidential Information

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to enable graceful restart:

```
RP/0/RP0/CPU0:router(config)# router bgp 3
RP/0/RP0/CPU0:router(config-bgp)# bgp graceful-restart
```

Related Commands

Command	Description
bgp graceful-restart graceful-reset	Enables a graceful reset if configuration changes force a peer reset.
bgp graceful-restart purge-time	Defines the maximum time before stale routes are purged.
bgp graceful-restart restart-time	Defines the maximum time advertised to neighbors
bgp graceful-restart stalepath-time	Defines the maximum time to wait for the End-of-RIB message from a neighbor that has been restarted before deleting learned routes.
show bgp	Displays entries in the BGP routing table.
show bgp neighbors	Displays information about BGP connections to neighbors.
show bgp process	Displays BGP process information.

R3.3 Beta Draft – Cisco Confidential Information

bgp graceful-restart graceful-reset

To invoke a graceful restart when configuration changes force a peer reset, use the **bgp graceful-restart graceful-reset** command in an appropriate configuration mode. To disable this function, use the **no** form of this command.

bgp graceful-restart graceful-reset

no bgp graceful-restart graceful-reset

Syntax Description This command has no arguments or keywords.

Defaults Graceful restart is not invoked when a configuration change forces a peer reset.

Command Modes Router configuration
VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

BGP graceful restart must be enabled using the **bgp graceful-restart** command before enabling graceful reset using the **bgp graceful-restart graceful-reset** command.

Task ID	Task ID	Operations
	bgp	read, write

Examples The following example shows how to enable graceful reset:

```
RP/0/RP0/CPU0:router(config)# router bgp 3  
RP/0/RP0/CPU0:router(config-bgp)# bgp graceful-restart graceful-reset
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	bgp graceful-restart	Enables a graceful restart.
	show bgp	Displays entries in the BGP routing table.
	show bgp neighbors	Displays information about BGP connections to neighbors.
	show bgp process	Displays BGP process information.

R3.3 Beta Draft—Cisco Confidential Information

bgp graceful-restart purge-time

To specify the maximum time before stale routes are purged from the routing information base (RIB) when the local BGP process restarts, use the **bgp graceful-restart purge-time** command in an appropriate configuration mode. To set the purge timer time to its default value, use the **no** form of this command.

bgp graceful-restart purge-time *seconds*

no bgp graceful-restart purge-time *seconds*

Syntax Description	<i>seconds</i>	Maximum time before stale routes are purged. Time in seconds. Range is 0 to 6000.

Defaults	<i>seconds</i> : 600

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

BGP graceful restart must be enabled using the **bgp graceful-restart** command before setting the purge time using the **bgp graceful-restart purge-time** command.

Task ID	Task ID	Operations
	bgp	read, write

Examples	The following example shows how to change the BGP purge time to 800 seconds:

```
RP/0/RP0/CPU0:router(config)# router bgp 3  
RP/0/RP0/CPU0:router(config-bgp)# bgp graceful-restart purge-time 800
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	bgp graceful-restart	Enables a graceful restart.
	show bgp	Displays entries in the BGP routing table.
	show bgp neighbors	Displays information about BGP connections to neighbors.
	show bgp process	Displays BGP process information.

R3.3 Beta Draft—Cisco Confidential Information

bgp graceful-restart restart-time

To specify a user-predicted local BGP process maximum restart time, which is advertised to neighbors during session establishment, use the **bgp graceful-restart restart-time** command in an appropriate configuration mode. To set this restart time to its default value, use the **no** form of this command.

bgp graceful-restart restart-time *seconds*

no bgp graceful-restart restart-time *seconds*

Syntax Description	<i>seconds</i>	Maximum time advertised to neighbors. Time in seconds. Range is 1 to 4095.

Defaults	<i>seconds</i> : 120

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. BGP graceful restart must be enabled using the bgp graceful-restart command before setting the restart timer using the bgp graceful-restart restart-time command.

Task ID	Task ID	Operations
	bgp	read, write

Examples	The following example shows how to change the BGP graceful restart time to 400 seconds: <pre>RP/0/RP0/CPU0:router(config)# router bgp 3 RP/0/RP0/CPU0:router(config-bgp)# bgp graceful-restart restart-time 400</pre>

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	bgp graceful-restart	Enables a graceful restart.
	show bgp	Displays entries in the BGP routing table.
	show bgp neighbors	Displays information about BGP connections to neighbors.
	show bgp process	Displays BGP process information.

R3.3 Beta Draft – Cisco Confidential Information

bgp graceful-restart stalepath-time

To specify the maximum time to wait for an End-of-RIB message after a neighbor restarts, use the **bgp graceful-restart stalepath-time** command in an appropriate configuration mode. To set the stalepath timer time to its default value, use the **no** form of this command.

bgp graceful-restart stalepath-time *seconds*

no bgp graceful-restart stalepath-time *seconds*

Syntax Description

<i>seconds</i>	Maximum wait time. Time in seconds. Range is 1 to 4095.

Defaults

seconds: 360

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

BGP graceful restart must be enabled using the **bgp graceful-restart** command before setting the stalepath time using the **bgp graceful-restart stalepath-time** command.

If the stalepath time is exceeded before an End-of-RIB message is received from a neighbor, paths learned from the neighbor are purged from the BGP routing table.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to change the stalepath time to 750 seconds:

```
RP/0/RP0/CPU0:router(config)# router bgp 3
RP/0/RP0/CPU0:router(config-bgp)# bgp graceful-restart stalepath-time 750
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	bgp graceful-restart	Enables a graceful restart.
	show bgp	Displays entries in the BGP routing table.
	show bgp neighbors	Displays information about BGP connections to neighbors.
	show bgp process	Displays BGP process information.

R3.3 Beta Draft—Cisco Confidential Information

bgp log neighbor changes disable

To disable logging of Border Gateway Protocol (BGP) neighbor resets, use the **bgp log neighbor changes disable** command in an appropriate configuration mode. To re-enable logging of BGP neighbor resets, use the **no** form of this command.

bgp log neighbor changes disable

no bgp log neighbor changes disable

Syntax Description

This command has no arguments or keywords.

Defaults

BGP neighbor changes are logged.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was first introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was first supported on the Cisco XR 12000 Series Router. The disable keyword was changed from optional to mandatory.
Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Logging of BGP neighbor status changes (up or down) and resets is used 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.

Status change message logging does not substantially affect performance, unlike, for example, enabling per-BGP update debugging. If the UNIX syslog facility is enabled, messages are sent by the software to the UNIX host running the syslog daemon so that the messages can be stored and archived on disk. If the UNIX syslog facility is not enabled, the status change messages are kept 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 disabled** command is disabled, except for the last reset reason, which is always available as output of the **show bgp neighbors** command.

Up and down messages for BGP neighbors are logged by the software by default. Use the **bgp log neighbor changes disable** command to stop logging BGP neighbor changes.

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

R3.3 Beta Draft – Cisco Confidential Information

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to prevent the logging of neighbor changes for BGP:

```
RP/0/RP0/CPU0:router(config)# router bgp 65530  
RP/0/RP0/CPU0:router(config-bgp)# bgp log neighbor change disable
```

Related Commands

Command	Description
logging buffered	Logs messages to an internal buffer.
show bgp neighbors	Displays information about the TCP and BGP connections to neighbors.
show logging	Displays the state of logging (syslog).

R3.3 Beta Draft—Cisco Confidential Information

bgp maximum neighbor

To control the maximum number of neighbors that can be configured on the router, use the **bgp maximum neighbor** command in an appropriate configuration mode. To set the neighbor limit to the default value, use the **no** form of this command.

bgp maximum neighbor *limit*

no maximum log neighbor *limit*

Syntax Description

<i>limit</i>	Maximum number of neighbors. Range is 1 to 15000.

Defaults

Default limit is 4000

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 3.2	This command was first supported on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Any attempt to configure the neighbor limit below 1 or above 1500 will fail. Similarly, attempt to configure the limit below the number of neighbor that is already configured will also fail.

Task ID

Task ID	Operations
bgp	write

Examples

The following example shows how to change the default maximum neighbor limit and set it to 1200:

```
RP/0/RP0/CPU0:router(config)# router bgp 65530  
RP/0/RP0/CPU0:router(config-bgp)# bgp maximum neighbor 1200
```

R3.3 Beta Draft—Cisco Confidential Information

bgp redistribute-internal

To allow the redistribution of internal Border Gateway Protocol (iBGP) routes into an Interior Gateway Protocol (IGP), such as Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF), use the **bgp redistribute-internal** command in an appropriate configuration mode. To disable the redistribution of iBGP routes 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

By default, iBGP routes are not redistributed into IGPs.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use of the **bgp redistribute-internal** command requires the **clear route *** command to be issued to reinstall all BGP routes into the IP routing table.



Note

Redistributing iBGP routes into IGPs may cause routing loops to form within an autonomous system. Use this command with caution.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to redistribute iBGP routes into OSPF:

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# bgp redistribute-internal
```

R3.3 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config-bgp)# exit
RP/0/RP0/CPU0:router(config)# router ospf area1
RP/0/RP0/CPU0:router(config-router)# redistribute bgp 1
RP/0/RP0/CPU0:router(config-router)# commit
```

Related Commands

Command	Description
clear bgp *	Resets all BGP neighbors.
clear route *	Resets all routes.

R3.3 Beta Draft—Cisco Confidential Information

bgp router-id

To configure a fixed router ID for a Border Gateway Protocol (BGP)-speaking router, use the **bgp router-id** command in an appropriate configuration mode. To disable a fixed route ID, use the **no** form of this command.

bgp router-id {*ip-address*}

no bgp router-id

Syntax Description

<i>ip-address</i>	IP Version 4 (IPv4) address to use as the router ID. Normally, this should be an IPv4 address assigned to the router.

Defaults

If no router ID is configured in BGP, BGP attempts to use the global router ID if one is configured and available. Otherwise, BGP uses the highest IP address configured on a loopback interface.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF configuration mode. The <i>interface-type interface-instance</i> arguments were removed.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If you do not use the **bgp router-id** command to configure a router ID, and an IP address is not configured on any loopback interface or no global router ID is configured, BGP neighbors remain down.

For more details on router IDs, see the *Cisco IOX XR Routing Configuration Guide*.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to configure the local router with the router ID of 192.168.70.24:

```
RP/0/RP0/CPU0:router(config)# router bgp 100
RP/0/RP0/CPU0:router(config-bgp)# bgp router-id 192.168.70.24
```

R3.3 Beta Draft—Cisco Confidential Information**Related Commands**

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

R3.3 Beta Draft—Cisco Confidential Information

bgp scan-time

To configure scanning intervals of Border Gateway Protocol (BGP)-speaking networking devices, use the **bgp scan-time** command in an appropriate configuration mode and address family configuration mode. To restore the scanning interval to its default value, use the **no** form of this command.

bgp scan-time *seconds*

no bgp scan-time

Syntax Description	<i>seconds</i>	Scanning interval (in seconds) of BGP routing information. Range is 5 to 3600 seconds.

Defaults	The default scanning interval is 60 seconds.

Command Modes	Router configuration IPv4 address family configuration IPv6 address family configuration VPNv4 address family configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in VPNv4 address family configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **bgp scan-time** command to change how frequently the software processes scanner tasks, such as conditional advertisement, dynamic MED changes, and periodic maintenance tasks.

Task ID	Task ID	Operations
	bgp	read, write

Examples	The following example shows how to set the scanning interval for IPv4 unicast to 20 seconds:

```
RP/0/RP0/CPU0:router(config)# router bgp 64500
RP/0/RP0/CPU0:router(config-bgp)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-af)# bgp scan-time 20
```

R3.3 Beta Draft—Cisco Confidential Information**Related Commands**

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

R3.3 Beta Draft—Cisco Confidential Information

bgp update-delay

To set the maximum initial delay for a Border Gateway Protocol (BGP)-speaking router to send the first updates, use the **bgp update-delay** command in an appropriate configuration mode. To restore the initial delay to its default value, use the **no** form of this command.

bgp update-delay *seconds* [**always**]

no bgp update-delay

Syntax Description

<i>seconds</i>	Delay in seconds for the router to send the first updates. Range is 0 to 3600.
always	(Optional) Specifies that the router always wait for the update delay time, even if all neighbors have finished sending their initial updates sooner.

Defaults

120 seconds

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When BGP is started, it waits a specified period of time for its neighbors to establish peering sessions and to complete sending their initial updates. After all neighbors complete their initial updates, or after the update delay timer expires, the best path is calculated for each route, and the software starts sending advertisements out to its peers. This behavior improves convergence time. If the software were to advertise a route as soon as it learned it, it would have to readvertise the route each time it learned a new path that was preferred over all previously learned paths.

Use the **bgp update-delay** command to tune the maximum time the software waits after the first neighbor is established until it starts calculating best paths and sending out advertisements.

Task ID

Task ID	Operations
bgp	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to set the maximum initial delay to 240 seconds:

```
RP/0/RP0/CPU0:router(config)# router bgp 64530  
RP/0/RP0/CPU0:router(config-bgp)# bgp update-delay 240
```

R3.3 Beta Draft—Cisco Confidential Information

bgp write-limit

To modify the upper bounds on update message queue lengths or to enable desynchronization, use the **bgp write-limit** command in an appropriate configuration mode. To return the bounds to their default values and to disable desynchronization, use the **no** form of this command.

bgp write-limit *group-limit global-limit* [**desynchronize**]

no bgp write-limit *group-limit global-limit* [**desynchronize**]

Syntax Description

<i>group-limit</i>	Per-update group limit on the number of update messages the software queues. Range is 500 to 100000000. Group limit cannot be greater than the global limit.
<i>global-limit</i>	Global limit on the number of update messages the software queues. Range is 500 to 100000000.
desynchronize	(Optional) Enables desynchronization.

Defaults

group-limit: 5000
global-limit: 25000
 Desynchronization is off.

Command Modes

Router configuration
 VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **bgp write-limit** command to configure both a per-update group and a global limit on the number of messages the software queues when updating peers. Increasing these limits can result in faster Border Gateway Protocol (BGP) convergence, but also may result in higher memory use during convergence. In addition, this command can be used to enable desynchronization. Desynchronization can decrease memory use and speed up convergence for the fastest neighbors if one or more neighbors in an update group process updates significantly slower than other neighbors in the same group. However, enabling desynchronization can cause a significant degradation in overall convergence time, especially if the router is experiencing high CPU utilization. For this reason, enabling desynchronization is discouraged.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	bgp	read, write

Examples

The following example shows how to configure BGP to operate with a per-update group limit of 9,000 messages and a global limit of 27,000 messages:

```
RP/0/RP0/CPU0:router(config)# router bgp 65000
RP/0/RP0/CPU0:router(config-bgp)# bgp write-limit 9000 27000
```

R3.3 Beta Draft—Cisco Confidential Information

capability orf prefix

To advertise prefix list-based Outbound Route Filter (ORF) capability to the Border Gateway Protocol (BGP) peer, use the **capability orf prefix** command in an appropriate configuration mode. To remove the **capability orf prefix** command from the configuration file and restore the system to its default condition in which the software does not advertise the capability, use the **no** form of this command.

capability orf prefix {receive | send | both | none}

no capability orf prefix

Syntax Description

receive	Sets the capability to receive the ORF from a specified neighbor.
send	Sets the capability to send the ORF to a specified neighbor.
both	Sets the capability to receive and send the ORF from or to a specified neighbor.
none	Sets the capability to no for ORF receive or send from or to a specified neighbor.

Defaults

The routing device does not receive or send route prefix filter lists.

Command Modes

IPv4 address family group configuration
 IPv6 address family group configuration
 IPv4 neighbor address family configuration
 VRF neighbor IPv4 address family configuration
 IPv4 neighbor group address family configuration
 IPv6 neighbor group address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was changed from capability orf prefix-list to capability orf prefix . This command was supported in VRF neighbor IPv4 address family configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information

The advertisement of the prefix list ORF capability by a BGP speaker indicates whether the speaker can send prefix lists to the specified neighbor and whether it accepts prefix lists from the neighbor. The speaker sends a prefix list if it indicated the ability to send them, and if the neighbor indicated it was willing to accept them. Similarly, the neighbor sends a prefix list to the speaker if it indicated the ability to send them and the speaker indicated the willingness to accept them.



Note

The `capability orf` and prefix list filter lists must be explicitly configured.

If the neighbor sends a prefix list and the speaker accepts it, the speaker applies the received prefix list, plus any locally configured outbound filters, to limit its outbound routing updates to the neighbor. Increased filtering prevents unwanted routing updates between neighbors and reduces resource requirements for routing update generation and processing.

Use the **capability orf prefix** command to set whether to advertise send and receive capabilities to the specified neighbor.



Note

Sending a receive capability can adversely affect performance because updates sent to that neighbor cannot be replicated for any other neighbors.

If this command is configured for a neighbor group or neighbor address family group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

Task ID

Task ID Operations

bgp	read, write

Examples

The following example shows the local BGP speaker advertising that the speaker is willing to accept an ORF prefix from its neighbor:

```
RP/0/RP0/CPU0: # configure
RP/0/RP0/CPU0: (config) # router bgp 65530
RP/0/RP0/CPU0: (config-bgp) # neighbor 10.0.101.1
RP/0/RP0/CPU0: (config-bgp-nbr) # remote-as 65534
RP/0/RP0/CPU0: (config-bgp-nbr) # address-family ipv4 unicast
RP/0/RP0/CPU0: (config-bgp-nbr-af) # capability orf prefix receive
```

The following example shows how to configure neighbor group orf to advertise ORF send capabilities:

```
RP/0/RP0/CPU0: # configure
RP/0/RP0/CPU0: (config) # router bgp 65530
RP/0/RP0/CPU0: (config-bgp) # neighbor-group orf
RP/0/RP0/CPU0: (config-bgp-nbr) # address-family ipv4 unicast
RP/0/RP0/CPU0: (config-bgp-nbr-af) # capability orf prefix send
```

The following example shows how to configure af-group orf to advertise ORF send and receive capabilities:

```
RP/0/RP0/CPU0: # configure
RP/0/RP0/CPU0: (config) # router bgp 65000
RP/0/RP0/CPU0: (config-bgp) # af-group orf address-family ipv4 unicast
RP/0/RP0/CPU0: (config-bgp-afgrp) # capability orf prefix both
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	af-group	Creates an address family group for BGP neighbors and enters address family group configuration mode.
	neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
	rd	Filters updates advertised to or received from a neighbor.
	show bgp neighbors	Displays information about BGP neighbors.

R3.3 Beta Draft—Cisco Confidential Information

clear bgp

To reset a group of Border Gateway Protocol (BGP) neighbors, use the **clear bgp** command in EXEC mode.

```
clear bgp [vpnv4 unicast | vrf {vrf-name | all} [ipv4 unicast]] [* | ip-address | as-number |
external] [graceful]
```

Syntax Description		
vpnv4 unicast	(Optional)	Specifies VPNv4 unicast address families.
vrf	(Optional)	Specifies VPN routing and forwarding (VRF).
<i>vrf-name</i>	(Optional)	Name of a VRF.
all	(Optional)	For VRF, specifies all VRFs.
ipv4 unicast	(Optional)	For VRF, specifies IPv4 unicast address families.
*		Resets all BGP neighbors.
<i>ip-address</i>		IP address of the neighbor to be reset.
<i>as-number</i>		Autonomous system number of neighbors to be reset. Range is 1 to 65535.
external		Specifies clearing of all external peers.
graceful	(Optional)	Specifies clearing with a hard reset and a graceful restart.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	The following keywords and arguments were added: vpnv4 unicast vrf <i>vrf-name</i> all ipv4 unicast

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information

Use the **clear bgp** command to reset the sessions of the specified group of neighbors (hard reset); it removes the TCP connection to the neighbor, removes all routes received from the neighbor from the BGP table, and then re-establishes the session with the neighbor.

If the **graceful** keyword is specified, the routes from the neighbor are not removed from the BGP table immediately, but are marked as stale. After the session is re-established, any stale route that has not been received again from the neighbor is removed.

Task ID

Task ID	Operations
bgp	execute

Examples

The following example shows how to hard reset neighbor 10.0.0.1:

```
RP/0/RP0/CPU0:router# clear bgp 10.0.0.1
```

The following example shows how to hard reset all neighbors with a graceful restart:

```
RP/0/RP0/CPU0:router# clear bgp * graceful
```

Related Commands

Command	Description
bgp bestpath as-path ignore	Enables an automatic soft reset of BGP peers when their configured route policy is modified.
clear bgp self-originated	Clears self-originated routes.
clear bgp soft	Soft resets a group of BGP neighbors.
show bgp	Displays entries in the BGP routing table.
show bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

R3.3 Beta Draft—Cisco Confidential Information

clear bgp dampening

To clear Border Gateway Protocol (BGP) route dampening information and unsuppress the suppressed routes, use the **clear bgp dampening** command in EXEC mode.

```
clear bgp {ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
          vpnv4 unicast | vrf {vrf-name | all} {ipv4 unicast}} dampening [ip-address/mask-length]
```

Syntax Description		
ipv4		Specifies IP Version 4 address prefixes.
unicast		Specifies unicast address prefixes.
multicast		Specifies multicast address prefixes.
all		For subaddress families, specifies prefixes for all subaddress families.
ipv6		Specifies IP Version 6 address prefixes.
all		For address family, specifies prefixes for all address families.
vpnv4 unicast		Specifies VPNv4 unicast address families.
vrf		Specifies VPN routing and forwarding (VRF).
<i>vrf-name</i>		Name of a VRF.
all		For VRF, specifies all VRFs.
ipv4 unicast		For VRF, specifies IPv4 unicast address families.
<i>ip-address</i>		(Optional) IP address of the network about which to clear dampening information.
<i>/mask-length</i>		(Optional) Network mask applied to the IP address.

Defaults If no IP address is specified, dampening information for all routes is cleared.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	The following keywords and arguments were added: • vpnv4 unicast • vrf • <i>vrf-name</i> • all • ipv4 unicast

■ clear bgp dampening

R3.3 Beta Draft – Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
bgp	execute

Examples

The following example shows how to clear the route dampening information for all 172.20.0.0/16 IPv4 multicast paths:

```
RP/0/RP0/CPU0:router# clear bgp ipv4 multicast dampening 172.20.0.0/16
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
show bgp dampened-paths	Displays BGP dampened routes.

R3.3 Beta Draft—Cisco Confidential Information

clear bgp flap-statistics

To clear Border Gateway Protocol (BGP) flap counts for a specified group of routes, use the **clear bgp flap-statistics** command in EXEC mode.

```
clear bgp {ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
  vpnv4 unicast | vrf {vrf-name | all} {ipv4 unicast} } flap-statistics [regexp regexp |
  route-policy route-policy-name | network/mask-length | ip-address]
```

Syntax Description	
ipv4	Specifies IP Version 4 address prefixes.
unicast	Specifies unicast address prefixes.
multicast	Specifies multicast address prefixes.
all	For subaddress families, specifies prefixes for all subaddress families.
ipv6	Specifies IP Version 6 address prefixes.
all	For address family, specifies prefixes for all address families.
vpnv4 unicast	Specifies VPNv4 unicast address families.
vrf	Specifies VPN routing and forwarding (VRF).
<i>vrf-name</i>	Name of a VRF.
all	For VRF, specifies all VRFs.
ipv4 unicast	For VRF, specifies IPv4 unicast address families.
regexp <i>regexp</i>	(Optional) Clears flap statistics for routes whose AS paths match the regular expression.
route-policy <i>route-policy-name</i>	(Optional) Clears flap statistics for the specific route policy.
<i>network</i>	(Optional) Network for which flap counts are to be cleared.
<i>/mask-length</i>	(Optional) Network mask of the network for which flap counts are to be cleared.
<i>ip-address</i>	(Optional) Neighbor address. Clears only flap statistics for routes received from this neighbor.

Defaults No default behavior or value

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Release	Modification
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The filter-list <i>access-list</i> keyword and argument were changed to route-policy <i>route-policy-name</i> .
Release 3.3	The following keywords and arguments were added: • vpn4 unicast • vrf • <i>vrf-name</i> • all • ipv4 unicast

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
bgp	execute

Examples

The following example shows how to clear the flap count for all routes (in all address families) originating in autonomous system 1:

```
RP/0/RP0/CPU0:router# clear bgp all all flap-statistics regexp _1$
```

The following example shows how to clear the flap count for all IPv4 unicast routes received from neighbor 172.20.1.1:

```
RP/0/RP0/CPU0:router# clear bgp ipv4 unicast flap-statistics 172.20.1.1
```

R3.3 Beta Draft—Cisco Confidential Information

clear bgp peer-drops

To clear the connection-dropped counter, use the **clear bgp peer-drops** command in EXEC mode.

```
clear bgp peer-drops [* | ip-address]
```

Syntax Description	*	Specifies all BGP neighbors.
	ip-address	IP address of a specific network neighbor.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	bgp	execute

Examples	The following example shows how to clear the connection-dropped counter for all BGP neighbors:

```
RP/0/RP0/CPU0:router# clear bgp peer-drops *
```

Related Commands	Command	Description
	show bgp neighbors	Displays information about BGP connections to neighbors.

R3.3 Beta Draft—Cisco Confidential Information

clear bgp performance-statistics

To clear the performance statistics for all address families, use the **clear bgp performance-statistics** command.

clear bgp performance-statistics

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	bgp	execute

Examples The following example shows how to clear the performance statistics for all address families:

```
RP/0/RP0/CPU0:router# clear bgp performance-statistics
```

R3.3 Beta Draft—Cisco Confidential Information

clear bgp self-originated

To clear Border Gateway Protocol (BGP) routes that are self-originated, use the **clear bgp self-originated** command in EXEC mode.

```
clear bgp {ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
vrf {vrf-name | all} {ipv4 unicast}} self-originated
```

Syntax Description		
ipv4		Specifies IP Version 4 address prefixes.
unicast		Specifies unicast address prefixes.
multicast		Specifies multicast address prefixes.
all		For subaddress families, specifies prefixes for all subaddress families.
ipv6		Specifies IP Version 6 address prefixes.
all		For address family, specifies prefixes for all address families.
vrf		Specifies VPN routing and forwarding (VRF).
<i>vrf-name</i>		Name of a VRF.
all		For VRF, specifies all VRFs.
ipv4 unicast		For VRF, specifies IPv4 unicast address families.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	The following keywords and arguments were added: vrf <i>vrf-name</i> all ipv4 unicast

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Self-originated routes are routes locally originated by the **network** command, **redistribute** command, or **aggregate-address** command.

 clear bgp self-originated

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	bgp	execute

Examples

The following example shows how to clear self-originated IPv4 routes:

```
RP/0/RP0/CPU0:router# clear bgp ipv4 unicast self-originated
```

Related Commands	Command	Description
	aggregate-address	Creates an aggregate entry in a BGP routing table.
	network (BGP)	Specifies a local network that the BGP routing process should originate and advertise to its neighbors.
	redistribute (BGP)	Redistributes routes from another routing protocol into BGP.

R3.3 Beta Draft—Cisco Confidential Information

clear bgp shutdown

To clear all Border Gateway Protocol (BGP) neighbors that shut down due to low memory, use the **clear bgp shutdown** command in EXEC mode.

```
clear bgp {ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
vpnv4 unicast | vrf {vrf-name | all} {ipv4 unicast}} shutdown
```

Syntax Description		
ipv4		Specifies IP Version 4 address prefixes.
unicast		Specifies unicast address prefixes.
multicast		Specifies multicast address prefixes.
all		For subaddress families, specifies prefixes for all subaddress families.
ipv6		Specifies IP Version 6 address prefixes.
all		For address family, specifies prefixes for all address families.
vpnv4 unicast		Specifies VPNv4 unicast address families.
vrf		Specifies VPN routing and forwarding (VRF).
<i>vrf-name</i>		Name of a VRF.
all		For VRF, specifies all VRFs.
ipv4 unicast		For VRF, specifies IPv4 unicast address families.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
	Release 3.3	The following keywords and arguments were added: • vpnv4 unicast • vrf • <i>vrf-name</i> • all • ipv4 unicast

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

 clear bgp shutdown

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	bgp	execute

Examples

The following example shows how to clear all shut-down BGP neighbors:

```
RP/0/RP0/CPU0:router# clear bgp shutdown
```

Related Commands

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

R3.3 Beta Draft – Cisco Confidential Information

clear bgp soft

To soft reset a group of Border Gateway Protocol (BGP) neighbors, use the **clear bgp soft** command in EXEC mode.

```
clear bgp { ipv4 { unicast | multicast | all } | ipv6 { unicast | all } | all { unicast | multicast | all } |
  vpnv4 unicast | vrf { vrf-name | all } { ipv4 unicast } } { * | ip-address | as-number | external }
  soft [in [prefix-filter] | out]
```

Syntax Description		
ipv4		Specifies IP Version 4 address prefixes.
unicast		Specifies unicast address prefixes.
multicast		Specifies multicast address prefixes.
all		For subaddress families, specifies prefixes for all subaddress families.
ipv6		Specifies IP Version 6 address prefixes.
all		For address family, specifies prefixes for all address families.
vpnv4 unicast		Specifies VPNv4 unicast address families.
vrf		Specifies VPN routing and forwarding (VRF).
<i>vrf-name</i>		Name of a VRF.
all		For VRF, specifies all VRFs.
ipv4 unicast		For VRF, specifies IPv4 unicast address families.
*		Resets all BGP neighbors.
<i>ip-address</i>		IP address of the neighbor to be reset.
<i>as-number</i>		Autonomous system number for all neighbors to be reset. Range is 1 to 65535.
external		Specifies clearing of all external peers.
in		(Optional) Triggers an inbound soft reset. If the in or out keyword is not specified, both inbound and outbound soft resets are triggered.
prefix-filter		(Optional) Specifies to send a new Outbound Route Filter (ORF) to the neighbor. Neighbor installs the new ORF and resend its routes.
out		(Optional) Triggers an outbound soft reset. If the in or out keyword is not specified, both inbound and outbound soft resets are triggered.

Defaults No default behavior or value

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Release	Modification
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	The following keywords and arguments were added: • vpn4 unicast • vrf • <i>vrf-name</i> • all • ipv4 unicast

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **clear bgp soft** command to trigger a soft reset of the specified address families for the specified group of neighbors. This command is useful if you change the inbound or outbound policy for the neighbors, or any other configuration that affects the sending or receiving of routing updates.

If an outbound soft reset is triggered, BGP resends all routes for the address family to the given neighbors.

If an inbound soft reset is triggered, BGP by default sends a REFRESH request to the neighbor, if the neighbor has advertised the ROUTE_REFRESH capability. To determine whether the neighbor has advertised the ROUTE_REFRESH capability, use the **show bgp neighbors** command, and look for the following line of output:

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

If the neighbor does not support route refresh, but the **soft-reconfiguration inbound** command is configured for the neighbor, then BGP uses the routes cached as a result of the **soft-reconfiguration inbound** command to perform the soft reset.

If you want BGP to use the cached routes even if the neighbor supports route refresh, you can use the **always** keyword when configuring the **soft-reconfiguration inbound** command.

If the neighbor does not support route refresh and the **soft-reconfiguration inbound** command is not configured, then inbound soft reset is not possible. In this case, an error is printed.



Note

By default, if the configuration for an inbound or outbound route policy is changed, BGP performs an automatic soft reset. Use the **bgp auto-policy-soft-reset disable** command to disable this behavior.

Task ID

Task ID	Operations
bgp	execute

Examples

The following example shows how to trigger an inbound soft clear for IPv4 unicast routes received from neighbor 10.0.0.1:

```
RP/0/RP0/CPU0:router# clear bgp ipv4 unicast 10.0.0.1 soft in
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	bgp bestpath as-path ignore	Enables an automatic soft reset of BGP peers when their configured route policies are modified.
	clear bgp	Resets a group of BGP neighbors.
	clear bgp self-originated	Clears self-originated routes.
	show bgp	Displays entries in the BGP routing table.
	show bgp neighbors	Displays information about the TCP and BGP connections to neighbors.
	soft-reconfiguration inbound	Configures the software to store updates received from a neighbor.

R3.3 Beta Draft—Cisco Confidential Information

default-information originate (BGP)

To allow origination of a default route to be redistributed into the Border Gateway Protocol (BGP) from another protocol, use the **default-information originate** command in an appropriate configuration mode. To disable this function, use the **no** form of this command.

default-information originate

no default-information originate

Syntax Description This command has no arguments or keywords.

Defaults BGP does not permit redistribution of a default route into BGP.

Command Modes Router configuration
VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **redistribute** command to redistribute routes from another protocol into BGP. By default, if these routes include the default route (0.0.0.0/0 for IPv4 or ::/0 for IPv6), the default route is ignored. Use the **default-information originate** command to change this behavior so that the default route is not ignored and is redistributed into BGP along with the other routes for the protocol being redistributed.

Task ID	Task ID	Operations
	bgp	read, write

Examples The following example shows how to configure BGP to redistribute the default route into BGP:

```
RP/0/RP0/CPU0:router(config)# router bgp 164
RP/0/RP0/CPU0:router(config-bgp)# default-information originate
```

R3.3 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	redistribute (BGP)	Redistributes the default route into BGP.

R3.3 Beta Draft—Cisco Confidential Information

default-metric (BGP)

To set default metric values for the Border Gateway Protocol (BGP), use the **default-metric** command in an appropriate configuration mode. To disable metric values, use the **no** form of this command.

default-metric *value*

no default-metric

Syntax Description	<i>value</i>	Default metric value appropriate for the specified routing protocol. Range is 1 to 429496729.

Defaults	A metric is not sent.

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **default-metric** command to set the Multi Exit Discriminator (MED) to advertise to peers for routes that do not already have a metric set (routes that were received with no MED attribute).

Task ID	Task ID	Operations
	bgp	read, write

Examples	The following example shows how to set the BGP default metric:

```
RP/0/RP0/CPU0:router(config)# router bgp 109
RP/0/RP0/CPU0:router(config-bgp)# default-metric 10
```


R3.3 Beta Draft—Cisco Confidential Information

default-originate

To cause a Border Gateway Protocol (BGP) speaker (the local router) to send the default route 0.0.0.0/0 to a neighbor for use as a default route, use the **default-originate** command in an appropriate configuration mode. To disable this function, use the **no** form of this command.

default-originate [**disable** | **route-policy** *route-policy-name*]

no default-originate

Syntax Description	disable	(Optional) Prevents the default-originate command characteristics from being inherited from a parent group.
	route-policy <i>route-policy-name</i>	(Optional) Specifies the name of a route policy. The route policy allows route 0.0.0.0 to be injected conditionally. IPv6 address family is supported.

Defaults The default route is not advertised to BGP neighbors.

Command Modes

- IPv4 neighbor address family configuration
- IPv4 neighbor group address family configuration
- IPv6 neighbor group address family configuration
- VRF neighbor configuration
- IPv4 address family group configuration
- IPv6 address family group configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The policy keyword was changed to route-policy .
	Release 3.3	This command was supported in VRF neighbor configuration mode.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **default-originate** command does not require the presence of the default route (0.0.0.0/0 for IPv4 or ::/0 for IPv6) in the local router. When the **default-originate** command is used with a route policy, the default route is advertised if any route in the BGP table matches the policy.

Task ID	Task ID	Operations
	bgp	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to unconditionally advertise the route 0.0.0.0/0 to the neighbor 172.20.2.3:

```
RP/0/RP0/CPU0:router(config)# router bgp 109
RP/0/RP0/CPU0:router(config-bgp)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.2.3
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 200
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# default-originate
```

The following example shows how to advertise the route 0.0.0.0/0 to the neighbor 172.20.2.3 only if a route exists in the BGP table that matches the route policy called default-default-policy:

```
RP/0/RP0/CPU0:router(config)# router bgp 109
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.2.3
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 200
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# default-originate route-policy
default-default-policy
```

Related Commands

Command	Description
default-information originate (BGP)	Allows the default route to be redistributed into BGP by another routing protocol.
af-group	Creates an address family group for BGP neighbors and enters address family group configuration mode.
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.

R3.3 Beta Draft – Cisco Confidential Information

description (BGP)

To annotate a neighbor, neighbor group, or session group, use the **description** command in an appropriate configuration mode. To remove the annotation, use the **no** form of this command.

description *text*

no description

Syntax Description

<i>text</i>	Meaningful description or comment.

Defaults

No comment or description exists.

Command Modes

Neighbor group configuration
Neighbor configuration
Session group configuration
VRF neighbor configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF neighbor configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **description** command to provide a description of a neighbor, neighbor group, or session group. The description is used to save user comments and does not affect software function.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to configure the description “Our best customer” on the neighbor 192.168.13.4:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router bgp 65000
RP/0/RP0/CPU0:router(config-bgp)# neighbor 192.168.13.4
RP/0/RP0/CPU0:router(config-bgp-nbr)# description Our best customer
```

R3.3 Beta Draft—Cisco Confidential Information

distance bgp

To allow the use of external, internal, and local administrative distances that could be used to prefer one class of routes over another, use the **distance bgp** command in an appropriate configuration mode. To disable the use of administrative distances, use the **no** form of this command.

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

no distance bgp

Syntax Description

<i>external-distance</i>	Administrative distance for Border Gateway Protocol (BGP) external routes. External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Range is 1 to 255. Routes with a distance of 255 are not installed in the routing table.
<i>internal-distance</i>	Administrative distance for BGP internal routes. Internal routes are those routes that are learned from another BGP entity within the same autonomous system. Range is 1 to 255. Routes with a distance of 255 are not installed in the routing table.
<i>local-distance</i>	Administrative distance for BGP local routes. The <i>local-distance</i> argument applies to locally generated aggregate routes (such as the routes generated by the aggregate-address command) and backdoor routes installed in the routing table. Range is 1 to 255. Routes with a distance of 255 are not installed in the routing table.

Defaults

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

Command Modes

IPv4 address family configuration
 IPv6 address family configuration
 VRF IPv4 address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF IPV4 address family configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information

Use the **distance bgp** command if another protocol is known to be able to provide a better route to a node than was actually learned using external BGP, or if some internal routes should be preferred by BGP.



Note

Changing the administrative distance of BGP internal routes is considered risky and is not recommended. One problem that can arise is the accumulation of routing table inconsistencies, which can interfere with routing.

An administrative distance is a rating of the trustworthiness of a routing information source. Numerically, an administrative distance is an 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.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows that iBGP routes are preferable to locally generated routes, so the administrative distance values are set accordingly:

```
RP/0/RP0/CPU0:router(config)# router bgp 109
RP/0/RP0/CPU0:router(config-bgp)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-af)# distance bgp 20 20 200
```

Related Commands

Command	Description
distance (IS-IS)	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
distance (OSPF)	Defines OSPF route administrative distances based on route type.

R3.3 Beta Draft—Cisco Confidential Information

dmz-link-bandwidth

To originate a demilitarized zone (DMZ) link bandwidth extended community for the link to an eBGP neighbor, use the **dmz-link-bw** command in an appropriate configuration mode. To cease origination of the DMZ link bandwidth extended community, use the **no** form of this command.

dmz-link-bandwidth [**disable**]

no dmz-link-bandwidth

Syntax Description	disable	(Optional) Prevents the dmz-link-bandwidth command from being inherited from a parent group.

Defaults	BGP does not originate the DMZ link bandwidth extended community.

Command Modes	Neighbor configuration Neighbor group configuration Session group configuration VRF neighbor configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The dmzlink-bw command was replaced with the dmz-link-bandwidth command.
	Release 3.3	This command was supported in VRF neighbor configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **dmz-link-bandwidth** command to advertise the bandwidth of links that are used to exit an autonomous system.

If this command is configured for a neighbor group or session group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

Task ID	Task ID	Operations
	bgp	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to advertise the bandwidth of links on router bgp 1:

```
RP/0/RP0/CPU0:router(config)# router bgp 1  
RP/0/RP0/CPU0:router(config-bgp)# neighbor 45.67.89.01  
RP/0/RP0/CPU0:router(config-bgp-nbr)# dmz-link-bandwidth
```

Related Commands

Command	Description
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
session-group	Creates a session group and enters session group configuration mode.

R3.3 Beta Draft—Cisco Confidential Information

ebgp-multihop

To accept and attempt Border Gateway Protocol (BGP) connections to external peers residing on networks that are not directly connected, use the **ebgp-multihop** command in an appropriate configuration mode. To disable connections to external peers and allow only direct connections between neighbors, use the **no** form of this command.

ebgp-multihop [*ttl-value*]

no ebgp-multihop

Syntax Description

<i>ttl-value</i>	(Optional) Time-to-live (TTL) value. Range is 1 to 255 hops.

Defaults

The external BGP (eBGP) multihop TTL default value is 1 if the **ebgp-multihop** command is not specified. If the command is specified but a TTL value is not given, the default is 1.

Command Modes

Neighbor configuration
VRF neighbor configuration
Neighbor group configuration
Session group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF neighbor configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **ebgp-multihop** command to enable multihop peerings with external BGP neighbors. The BGP protocol states that external neighbors must be directly connected (one hop away). The software enforces this by default; however, the **ebgp-multihop** command can be used to override this behavior.

If this command is configured for a neighbor group or session group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

Task ID

Task ID	Operations
bgp	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to allow a BGP connection to neighbor 172.20.16.6 of up to 255 hops away:

```
RP/0/RP0/CPU0:router(config)# router bgp 109  
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.16.6  
RP/0/RP0/CPU0:router(config-bgp-nbr)# ebgp-multihop
```

Related Commands

Command	Description
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
session-group	Creates a session group and enters session group configuration mode.

R3.3 Beta Draft—Cisco Confidential Information

export route-policy

To configure an export route policy, use the **export route-policy** command in global VRF IPv4 address family configuration mode. To restore the system to its default condition, use the **no** form of this command.

export route-policy *policy-name*

no export route-policy *policy-name*

Syntax Description	<i>policy-name</i>	Name of the configured route policy.

Defaults	No default behavior or values

Command Modes	Global VRF IPv4 address family configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the export route-policy command define the conditions that allow specified routes to be tagged with specified route-targets.

Task ID	Task ID	Operations
	bgp	read, write
	ip-services	read, write

Examples	The following example shows how to configure an export route policy:
	RP/0/RP0/CPU0:router(config)# vrf vrf-1
	RP/0/RP0/CPU0:router(config-vrf)# address-family ipv4 unicast
	RP/0/RP0/CPU0:router(config-vrf-af)# export route-policy policy-A

Related Commands	Command	Description
	import route-policy	Imports a selected route policy into the VRF instance.

R3.3 Beta Draft—Cisco Confidential Information

export route-target

To configure a VPN routing and forwarding (VRF) export route-target extended community, use the **export route-target** command in global VRF IPv4 address family configuration mode. To restore the system to its default condition, use the **no** form of this command.

export route-target [*as-number:nn* | *ip-address:nn*]

no export route-target [*as-number:nn* | *ip-address:nn*]

Syntax Description

<i>as-number:nn</i>	(Optional) Autonomous system (AS) number of the route-target extended community. <i>as-number</i>—16-bit AS number <i>nn</i>—32-bit number
<i>ip-address:nn</i>	(Optional) IP address of the route-target extended community. <i>ip-address</i>—32-bit IP address <i>nn</i>—16-bit number

Defaults

No default behavior or values

Command Modes

Global VRF IPv4 address family configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Export route-target extended communities are associated with prefixes when advertised to remote provider edge (PE) routers. The remote PE routers import the route-target extended communities into a VRF instance that has the import route-targets that match the exported route-target extended communities.

Task ID

Task ID	Operations
bgp	read, write
ip-services	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to specify an export route-target:

```
RP/0/RP0/CPU0:router(config)# vrf vrf-1  
RP/0/RP0/CPU0:router(config-vrf)# address-family ipv4 unicast  
RP/0/RP0/CPU0:router(config-vrf-af)# export route-target 500:1
```

Related Commands

Command	Description
import route-target	Specifies the import route-target.

R3.3 Beta Draft—Cisco Confidential Information

import route-policy

To configure an import route policy, use the **import route-policy** command in global VRF IPv4 address family configuration mode. To restore the system to its default condition, use the **no** form of this command.

import route-policy *policy-name*

no import route-policy *policy-name*

Syntax Description

<i>policy-name</i>	Name of the configured route policy.

Defaults

No default behavior or values

Command Modes

Global VRF IPv4 address family configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **import route-policy** command to define the conditions that allow specified routes to be imported into the VPN routing and forwarding (VRF) instance if the routes are tagged with specified route-targets.

Task ID

Task ID	Operations
bgp	read, write
ip-services	read, write

Examples

The following example shows how to allow only policy-B to be imported to VRF:

```
RP/0/RP0/CPU0:router(config)# vrf vrf-1
RP/0/RP0/CPU0:router(config-vrf)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-vrf-af)# import route-policy policy-B
```

Related Commands

Command	Description
export route-policy	Exports a selected route policy into the VRF instance.

R3.3 Beta Draft—Cisco Confidential Information

import route-target

To configure a VPN routing and forwarding (VRF) import route-target extended community, use the **import route-target** command in global VRF IPv4 address family configuration mode. To restore the system to its default condition, use the **no** form of this command.

import route-target [*as-number:nn* | *ip-address:nn*]

no import route-target [*as-number:nn* | *ip-address:nn*]

Syntax Description

<i>as-number:nn</i>	(Optional) Autonomous system (AS) number of the route-target extended community. <i>as-number</i>—16-bit AS number <i>nn</i>—32-bit number
<i>ip-address:nn</i>	(Optional) IP address of the route-target extended community. <i>ip-address</i>—32-bit IP address <i>nn</i>—16-bit number

Defaults

No default behavior or values

Command Modes

Global VRF IPv4 address family configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **import route-target** command to specify that prefixes associated with the configured import route-target extended communities are imported into the VPN routing and forwarding (VRF) instance.

Task ID

Task ID	Operations
bgp	read, write
ip-services	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to specify an import route-target:

```
RP/0/RP0/CPU0:router(config)# vrf vrf-1
RP/0/RP0/CPU0:router(config-vrf)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-vrf-af)# import route-target 500:99
```

Related Commands

Command	Description
export route-target	Specifies the export route-target.

R3.3 Beta Draft—Cisco Confidential Information

label-allocation-mode

To set the MPLS/VPN label allocation mode, use the **label-allocation-mode** command in VRF configuration mode. To remove the **label-allocation-mode** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

label-allocation-mode per-ce

no label-allocation-mode per-ce

Syntax Description	per-ce	Specifies that the same label is used for all the routes advertised from a unique customer edge (CE).

Defaults	Per-prefix is the default label allocation mode.

Command Modes	VRF configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Each prefix that belongs to a VRF instance is advertised with a single label, causing an additional lookup to be performed in the VRF forwarding table to determine the customer edge (CE) next-hop for the packet. Use the **label-allocation-mode** command with the **per-ce** keyword to avoid the additional lookup on the PE router and conserve label space. This mode allows the PE router to allocate one label for every immediate next-hop. The label is directly mapped to the next-hop so there is no VRF route lookup performed during data forwarding. However, the number of labels allocated is one for each CE rather than one for each VRF.

Task ID	Task ID	Operations
	bgp	read, write

Examples	The following example shows how to set the label allocation mode to customer edge:

```
RP/0/RP0/CPU0:router(config)# router bgp 109
RP/0/RP0/CPU0:router(config-bgp)# vrf vrf-1
RP/0/RP0/CPU0:router(config-bgp-vrf)# label-allocation-mode per-ce
```


R3.3 Beta Draft—Cisco Confidential Information

local-as

To allow customization of the autonomous system number for external Border Gateway Protocol (eBGP) neighbor peerings, use the **local-as** command in an appropriate configuration mode. To disable customization of local autonomous system values for eBGP neighbor peerings, use the **no** form of this command.

local-as { *autonomous-system-number* [**no-prepend**] | **disable** }

no local-as [*autonomous-system-number* [**no-prepend**] | **disable**]

Syntax Description

<i>autonomous-system-number</i>	Valid autonomous system number. Range is 1 to 65535. Cannot be the autonomous system number to which the neighbor belongs.
no-prepend	(Optional) Specifies that local autonomous system values are not prepended to announcements from the neighbor.
disable	Disables the functionality of the command.

Defaults

The BGP autonomous system number specified in the **router bgp** command is used, except when confederations are in use. The confederation autonomous system is used for external neighbors in an autonomous system that is not part of the confederation.

Command Modes

Neighbor configuration
VRF neighbor configuration
Neighbor group configuration
Session group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The no-prepend and disable keywords were added.
Release 3.3	This command was supported in VRF neighbor configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You can specify the autonomous system number the local BGP uses to peer with each neighbor. The autonomous system number specified with this command cannot be the local BGP autonomous system number (specified with the **router bgp** command) or the autonomous system number of the neighbor (specified with the **remote-as** command). This command cannot be specified for internal neighbors or for external neighbors in an autonomous system that is part of a confederation.

R3.3 Beta Draft—Cisco Confidential Information

If this command is configured for a neighbor group or session group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

Task ID	Task ID	Operations
	bgp	read, write

Examples

The following example shows BGP using autonomous system 30 for the purpose of peering with neighbor 172.20.1.1:

```
RP/0/RP0/CPU0:router(config)# router bgp 140
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 300
RP/0/RP0/CPU0:router(config-bgp-nbr)# local-as 30
```

Related Commands

Command	Description
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
session-group	Creates a session group and enters session group configuration mode.

R3.3 Beta Draft—Cisco Confidential Information

maximum-paths (BGP)

To control the maximum number of parallel routes that Border Gateway Protocol (BGP) installs in the routing table, use the **maximum-paths** command in an appropriate configuration mode. To set the maximum number of parallel routes the software installs to the default value, use the **no** form of this command.

maximum-paths { **ebgp** | **ibgp** | **eibgp** } *maximum* [**unequal-cost**]

no maximum-paths { **ebgp** | **ibgp** | **eibgp** } *maximum* [**unequal-cost**]

Syntax Description

ebgp	Specifies external BGP multipath peers.
ibgp	Specifies internal BGP multipath peers.
eibgp	Specifies internal and external BGP multipath peers.
<i>maximum</i>	Maximum number of parallel routes that BGP installs in the routing table. Range is 2 to 8
unequal-cost	(Optional) Allows iBGP multipaths to have different BGP next-hop Interior Gateway Protocol (IGP) metrics. This option is available when the ibgp keyword is used.

Defaults

One path is installed in the routing table.

Command Modes

IPv4 address family configuration
IPv6 address family configuration
VRF IPv4 address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The ebgp and ibgp keywords were added and the <i>maximum</i> range was changed from 1–8 to 2–8.
Release 3.3	This command was supported in VRF IPv4 address family configuration mode. The eibgp and unequal-cost keywords were added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **maximum-paths** command to allow the BGP protocol to install multiple paths into the routing table for each prefix. Multiple paths are installed for external peers that are from the same autonomous system and are equal cost (according to the BGP best path algorithm). Similarly, multiple paths are installed for internal peers that are equal based on the BGP best path algorithm and the IGP metric to the

R3.3 Beta Draft—Cisco Confidential Information

BGP next hop is the same as the best path IGP metric unless the router is configured for unequal cost iBGP multipath. See *Implementing BGP on Cisco IOS XR Software* in the *Cisco IOS XR Routing Configuration Guide* for information on the BGP best path algorithm.

**Note**

The **maximum-paths** command with the **eibgp** keyword cannot be configured if the **ibgp** or **ebgp** keywords have been configured, because the **eibgp** keyword is a superset of the **ibgp** or **ebgp** keywords.

Task ID**Task ID Operations**

bgp	read, write

Examples

The following example shows how to allow a maximum of four paths to a destination installed into the IPv4 unicast routing table:

```
RP/0/RP0/CPU0:router(config)# router bgp 109  
RP/0/RP0/CPU0:router(config-bgp)# address-family ipv4 unicast  
RP/0/RP0/CPU0:router(config-bgp-af)# maximum-paths ebgp 4
```

R3.3 Beta Draft – Cisco Confidential Information

maximum-prefix (BGP)

To control how many prefixes can be received from a neighbor, use the **maximum-prefix** command in an appropriate configuration mode. To set the prefix limits to the default values, use the **no** form of this command.

maximum-prefix *maximum* [*threshold*] [**warning-only**]

no maximum-prefix

Syntax Description

<i>maximum</i>	Maximum number of prefixes allowed from this neighbor. Range is 1 to 4294967295.
<i>threshold</i>	(Optional) Integer specifying at what percentage of the <i>maximum</i> argument value the software starts to generate a warning message. Range is 1 to 100.
warning-only	(Optional) Instructs the software to generate a log message only when the maximum argument value is exceeded, and not terminate the peering.

Defaults

When this command is not specified, the following defaults apply:

IPv4 unicast: 524,288 prefixes

IPv4 multicast: 131,072 prefixes

IPv6 unicast: 131,072 prefixes

IPv6 multicast: 131,072 prefixes

VPNv4 unicast: 524, 288

The default threshold when a warning message is generated is 75 percent.

Command Modes

IPv4 address family group configuration
 IPv6 address family group configuration
 VPNv4 address family group configuration
 IPv4 neighbor address family configuration
 VPNv4 neighbor address family configuration
 IPv4 neighbor group address family configuration
 IPv6 neighbor group address family configuration
 VPNv4 neighbor group address family configuration
 VRF neighbor configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VPNv4 address family, VPNv4 neighbor address, and VPNv4 neighbor group address family, and VRF neighbor configuration modes.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **maximum-prefix** command to configure a maximum number of prefixes that a BGP router is allowed to receive from a neighbor. It adds another mechanism (besides routing policy) to control prefixes received from a peer.

When the number of received prefixes exceeds the maximum number configured, the software terminates the peering, by default, after sending a cease notification to the neighbor. However, if the **warning-only** keyword is configured, the software writes only a log message, but continues peering with the sender. If the peer is terminated, the peer stays down until the **clear bgp** command is issued.

This command takes effect immediately if configured on an established neighbor unless the number of prefixes received from the neighbor already exceeds the configured limits.

If this command is configured for a neighbor group or neighbor address family group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows the maximum number of IP Version 4 (IPv4) unicast prefixes allowed from the neighbor at 192.168.40.24 set to 1000:

```
RP/0/RP0/CPU0:router(config-bgp)# router bgp 109
RP/0/RP0/CPU0:router(config-bgp)# neighbor 192.168.40.24
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# maximum-prefix 1000
```

Related Commands

Command	Description
af-group	Creates an address family group for BGP neighbors and enters address family group configuration mode.
clear bgp	Resets a BGP connection using BGP hard or soft reconfiguration.
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.

R3.3 Beta Draft—Cisco Confidential Information

neighbor (BGP)

To enter neighbor configuration mode for configuring Border Gateway Protocol (BGP) routing sessions, use the **neighbor** command in an appropriate configuration mode. To delete all configuration for a neighbor and terminate peering sessions with the neighbor, use the **no** form of this command.

neighbor *ip-address*

no neighbor *ip-address*

Syntax Description	<i>ip-address</i>	IPv4 or IPv6 IP address of the BGP-speaking neighbor.

Defaults	Neighbor mode is not specified.

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

From router configuration mode, you can use this command to enter neighbor configuration mode.

From neighbor configuration mode, you can enter address family configuration for the neighbor by using the **address-family** command, which allows you to configure routing sessions for IP Version 4 and IP Version 6 address prefixes.

The **neighbor** command does not cause the neighbor to be configured and does not result in a peering to be established with the neighbor. To create the neighbor, you configure a remote autonomous system number by entering the **remote-as** command, or the neighbor can inherit a remote autonomous system from a neighbor group or session group if the **use** command is applied.

Unlike IPv4, IPv6 must be enabled before any IPv6 neighbors can be defined. Enable IPv6 in router configuration mode using the **address-family** command.



Note

Configuration for the neighbor cannot occur until the neighbor is given a remote autonomous system.

The **no** form of this command causes the peering with the neighbor to be terminated and all configuration that relates to the neighbor to be removed.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	bgp	read, write

Examples

The following example shows how to place the router in neighbor configuration mode for BGP routing process 1 and configure the neighbor IP address 172.168.40.24 as a BGP peer:

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.168.40.24
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 65000
```

The following example shows how to enable IPv6 for BGP, then place the router in neighbor configuration mode for an IPv6 neighbor, 3000::1, and configure neighbor 3000::1 as a BGP peer:

```
RP/0/RP0/CPU0:router(config)# router bgp 100
RP/0/RP0/CPU0:router(config-bgp)# address-family ipv6 unicast
RP/0/RP0/CPU0:router(config-bgp-af)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 3000::1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 2002
```

Related Commands

Command	Description
address-family (BGP)	Enters address family configuration mode for configuring BGP routing sessions.
remote-as (BGP)	Adds an entry to the BGP neighbor table.
use	Inherits characteristics from a neighbor group, session group, or address family group.

R3.3 Beta Draft—Cisco Confidential Information

neighbor-group

To create a neighbor group and enter neighbor group configuration mode, use the **neighbor-group** command in router configuration mode. To remove a neighbor group and delete all configuration associated with the group, use the **no** form of this command.

neighbor-group *name*

no neighbor-group *name*

Syntax Description

<i>name</i>	Neighbor group name.

Defaults

No neighbor group mode is specified.

Command Modes

Router configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **neighbor-group** command puts the router in neighbor group configuration mode and creates a neighbor group.

A neighbor group helps you apply the same configuration to one or more neighbors. After a neighbor group is configured, each neighbor can inherit the configuration through the **use** command. If a neighbor is configured to use a neighbor group, the neighbor, by default, inherits the entire configuration of the neighbor group, which includes the address family-independent and address family-specific configurations. The inherited configuration can be overridden if you directly configure commands for the neighbor or if you configure session groups or address family groups with the **use** command.

From neighbor group configuration mode, you can configure address family-independent parameters for the neighbor group. To enter address family-specific configuration for the neighbor group, use the **address-family** command when in the neighbor group configuration mode.



Note

If an address family is configured for a neighbor group, neighbors that use the neighbor group attempt to exchange routes in that address family.

R3.3 Beta Draft—Cisco Confidential Information

The **no** form of this command ordinarily causes all configuration for the neighbor group to be removed. If using the **no** form would result in a neighbor losing its remote autonomous system number, the configuration is rejected. In this scenario, the neighbor configuration must be either removed or configured with a remote autonomous system number before the neighbor group configuration can be removed.



Note

Neighbor groups should not be configured with a mixture of IPv4 and IPv6 address families, because such a neighbor group is not usable by any neighbor. Note that within the Cisco IOS XR system configuration architecture, it is possible to create such a neighbor group; however, any attempt to use it is rejected.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to create a neighbor group called group1 that has IP Version 4 (IPv4) unicast and IPv4 multicast activated along with various configuration features. The neighbor group is used by neighbor 10.0.0.1 and neighbor 10.0.0.2, which allows them to inherit the entire group1 configuration.

```
RP/0/RP0/CPU0:router(config)# router bgp 65530
RP/0/RP0/CPU0:router(config-bgp)# neighbor-group group1
RP/0/RP0/CPU0:router(config-bgp-nbrgrp)# remote-as 65535
RP/0/RP0/CPU0:router(config-bgp-nbrgrp)# advertisement-interval 2
RP/0/RP0/CPU0:router(config-bgp-nbrgrp)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbrgrp-af)# send-community-ebgp
RP/0/RP0/CPU0:router(config-bgp-nbrgrp-af)# exit
RP/0/RP0/CPU0:router(config-bgp-nbrgrp)# address-family ipv4 multicast
RP/0/RP0/CPU0:router(config-bgp-nbrgrp-af)# next-hop-self
RP/0/RP0/CPU0:router(config-bgp-nbrgrp-af)# exit
RP/0/RP0/CPU0:router(config-bgp-nbrgrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.0.0.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# use neighbor-group group1
RP/0/RP0/CPU0:router(config-bgp-nbr)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.0.0.2
RP/0/RP0/CPU0:router(config-bgp-nbr)# use neighbor-group group1
RP/0/RP0/CPU0:router(config-bgp-nbr)# exit
```

Related Commands

Command	Description
address-family (BGP)	Enters various address family configuration modes for configuring BGP routing sessions.
neighbor (BGP)	Enters neighbor configuration mode for configuring BGP routing sessions.
use	Inherits characteristics from a neighbor group, a session group, or an address family group.

R3.3 Beta Draft—Cisco Confidential Information

network (BGP)

To specify that the Border Gateway Protocol (BGP) routing process should originate and advertise a local network to its neighbors, use the **network** command in an appropriate configuration mode. To disable originating or advertising the network to neighbors, use the **no** form of this command.

network {*ip-address/prefix-length* | *ip-address mask*} [**route-policy** *route-policy-name*]

no network {*ip-address/prefix-length* | *ip-address mask*}

Syntax Description

<i>ip-address</i>	Network that BGP advertises.
<i>/prefix-length</i>	Length of the IP address prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash (/) must precede the decimal value.
<i>ip-address mask</i>	Network mask applied to the <i>ip-address</i> argument.
route-policy <i>route-policy-name</i>	(Optional) Specifies a route policy to use to modify the attributes of the network.

Defaults

No networks are specified.

Command Modes

IPv4 address family configuration
IPv6 address family configuration
VRF IPv4 address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The policy keyword was changed to route-policy .
Release 3.3	This command was supported in VRF IPv4 address family configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Although most Interior Gateway Protocols (IGPs) use the **network** command to indicate the interfaces on which the routing protocol runs, the **network** command in BGP determines which local networks are originated by this router. A network specified with this command is originated and advertised to neighbors only if there exists an IGP route for the network in the routing table. That is, there must be a route learned using local or connected networks, static routing, or a dynamic IGP such as IS-IS or OSPF.

R3.3 Beta Draft – Cisco Confidential Information

Other than the available system resources on the router, no limit exists on the number of network commands that can be configured.

Task ID	Task ID	Operations
	bgp	read, write

Examples

The following example shows how to configure the local router to originate the IPv4 unicast network 172.20.0.0/16:

```
RP/0/RP0/CPU0:router(config)# router bgp 120
RP/0/RP0/CPU0:router(config-bgp)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-af)# network 172.20.0.0/16
```

Related Commands	Command	Description
	network backdoor	Specifies a backdoor route to a BGP border router that provides better information about the network.
	redistribute (BGP)	Redistributes routes from one routing domain into another routing domain.

R3.3 Beta Draft—Cisco Confidential Information

network backdoor

To set the administrative distance on an external Border Gateway Protocol (eBGP) route to that of a locally sourced BGP route, causing it to be less preferred than an Interior Gateway Protocol (IGP) route, use the **network backdoor** command in an appropriate configuration mode. To disable setting the administrative distance to the value for locally sourced BGP routes, use the **no** form of this command.

network {*ip-address/prefix-length* | *ip-address mask*} **backdoor**

no network {*ip-address/prefix-length* | *ip-address mask*} **backdoor**

Syntax Description	<i>ip-address</i>	Network that provides a backdoor route.
	<i>/prefix-length</i>	Length of the IP address prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash (/) must precede the decimal value.
	<i>mask</i>	Network mask applied to the <i>ip-address</i> argument.

Defaults No backdoor routes are installed.

Command Modes IPv4 address family configuration
IPv6 address family configuration
VRF IPv4 address family configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in VRF IPv4 address family configuration mode.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Configuring the **network backdoor** command does not cause BGP to originate a network, even if an IGP route for the network exists. Ordinarily, the backdoor network would be learned through both an eBGP and IGP. The BGP best path selection algorithm does not change when a network is configured as a backdoor network.

Task ID	Task ID	Operations
	bgp	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows IP Version 4 (IPv4) unicast network 192.168.40.0/24 configured as a backdoor network:

```
RP/0/RP0/CPU0:router(config)# router bgp 109  
RP/0/RP0/CPU0:router(config-bgp)# address-family ipv4 unicast  
RP/0/RP0/CPU0:router(config-bgp-af)# network 192.168.40.0/24 backdoor
```

Related Commands

Command	Description
network (BGP)	Specifies a local network that the BGP routing process should originate and advertise to its neighbors.

R3.3 Beta Draft—Cisco Confidential Information

next-hop-self

To disable next-hop calculation and insert your own address in the next-hop field of Border Gateway Protocol (BGP) updates, use the **next-hop-self** command in an appropriate configuration mode. To enable next-hop calculation, use the **no** form of this command.

next-hop-self [disable]

no next-hop-self

Syntax Description

disable	(Optional) Allows next hop calculation override when this feature may be inherited from a neighbor group or address family group.

Defaults

When this command is not specified, the software calculates the next hop for BGP updates accepted by the router.

Command Modes

IPv4 address family group configuration
IPv6 address family group configuration
VPNv4 address family group configuration
IPv4 neighbor address family configuration
VPNv4 neighbor address family configuration
IPv4 neighbor group address family configuration
IPv6 neighbor group address family configuration
VPNv4 neighbor group address family configuration
VRF neighbor configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command is supported in the following configuration modes: • VPNv4 address family group • VPNv4 neighbor address family • VPNv4 neighbor group address family • VRF neighbor

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **next-hop-self** command to set the BGP next hop attribute of routes being advertised over a peering session to the local source address of the session.

R3.3 Beta Draft—Cisco Confidential Information

This command is useful in nonmeshed 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 this command is configured for a neighbor group or address family group, a neighbor using the group inherits the configuration. Configuring the command specifically for a neighbor overrides any inherited value.

Task ID	Task ID	Operations
	bgp	read, write

Examples

The following example shows how to set the next hop of the update field for all IP Version 4 (IPv4) unicast routes advertised to neighbor 172.20.1.1 to an address of the local router:

```
RP/0/RP0/CPU0:router(config)# router bgp 140
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# next-hop-self
```

The following example shows how to disable the **next-hop-self** command for neighbor 172.20.1.1. If not overridden, the next hop would be inherited from address family group group1:

```
RP/0/RP0/CPU0:router(config)# router bgp 140
RP/0/RP0/CPU0:router(config-bgp)# af-group group1 address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-afgrp)# next-hop-self
RP/0/RP0/CPU0:router(config-bgp-afgrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# use af-group group1
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# next-hop-self disable
```

Related Commands	Command	Description
	af-group	Creates an address family group for BGP neighbors and enters address family group configuration mode.
	neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
	use	Inherits characteristics from a neighbor group, session group, or address family group.

R3.3 Beta Draft—Cisco Confidential Information**orf**

To specify Outbound Route Filter (ORF) and inbound filtering criteria, use the **orf route-policy** command in an appropriate configuration mode. To restore the system to its default condition, use the **no** form of this command.

orf route-policy *route-policy-name*

no orf route-policy *route-policy-name*

Syntax Description

<i>route-policy-name</i>	Name of the route policy.

Defaults

No ORF route policy is defined.

Command Modes

IPv4 address family group configuration
 IPv6 address family group configuration
 IPv4 neighbor address family configuration
 VRF IPv4 neighbor address family configuration
 IPv4 neighbor group address family configuration
 IPv6 neighbor group address family configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to configure outbound and inbound filtering criteria:

```
RP/0/RP0/CPU0:router(config)# router bgp 6
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# orf route-policy policy_A
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	route-policy (BGP)	Applies a routing policy to updates advertised to or received from a BGP neighbor.

R3.3 Beta Draft—Cisco Confidential Information

password

To enable Message Digest 5 (MD5) authentication on a TCP connection between two Border Gateway Protocol (BGP) neighbors, use the **password** command in an appropriate configuration mode. To disable MD5 authentication, use the **no** form of this command.

password { **clear** | **encrypted** } *password*

no password [**clear** *password* | **encrypted** *password*]

Syntax Description

clear	Specifies that an unencrypted password follows. The password must be a case-sensitive, clear-text unencrypted password.
encrypted	Specifies that an encrypted password follows. The password must be a case-sensitive, encrypted password.
<i>password</i>	Password of up to 80 characters. The password can contain any alphanumeric characters. However, if the first character is a number or the password contains a space, the password must be enclosed in double quotation marks; for example, "2 password."

Defaults

When this command is not specified in the appropriate configuration mode, MD5 authentication is not enabled on a TCP connection between two BGP neighbors.

Command Modes

Neighbor configuration
VRF neighbor configuration
Neighbor group configuration
Session group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The 0 and 7 keywords were replaced with the clear and encrypted keywords and the accept keyword was removed.
Release 3.3	This command was supported in VRF neighbor configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Configure a password to enable authentication between two BGP peers. Use the **password** command to verify each segment sent on the TCP connection between the peers. The same password must be configured on both networking devices, otherwise a connection cannot be made. The authentication feature uses the MD5 algorithm. Specifying this command causes the software to generate and check the MD5 digest on every segment sent on the TCP connection.

R3.3 Beta Draft—Cisco Confidential Information

Configuring a neighbor password does not cause the existing session for a neighbor to end. However, until the new password is configured on the remote router, the local BGP process does not receive keepalive messages from the remote device. If the password is not updated on the remote device by the end of the hold time, the session ends. The hold time can be changed using the **timers** command or the **timers bgp** command.

If this command is configured for a neighbor group or neighbor address family group, a neighbor using the group inherits the configuration. Values of commands configured specifically for a neighbor overrides inherited values.

Task ID	Task ID	Operations
	bgp	read, write

Examples

The following example shows how to configure neighbor 172.20.1.1 to use MD5 authentication with the password password1:

```
RP/0/RP0/CPU0:router(config)# router bgp 140
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# password clear password1
```

Related Commands

Command	Description
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
password-disable	Overrides any inherited password configuration from a neighbor group or session group for BGP neighbors.
session-group	Creates a session group and enters session group configuration mode.
timers (BGP)	Set the timers for a specific BGP neighbor.

R3.3 Beta Draft—Cisco Confidential Information

password-disable

To override any inherited password configuration from a neighbor group or session group for Border Gateway Protocol (BGP) neighbors, use the **password-disable** command in an appropriate configuration mode. To disable overriding any inherited password command, use the **no** form of this command.

password-disable

no password-disable

Syntax Description

This command has no arguments or keywords.

Defaults

Configured passwords for neighbor and session groups are inherited.

Command Modes

Neighbor configuration
VRF neighbor configuration
Neighbor group configuration
Session group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF neighbor configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If you specify a password on a neighbor group or session group, all users of the group inherit the password. Specifying a different **password** command specifically on a neighbor that uses the group overrides the inherited value. Specifying **password-disable** on a neighbor that uses the group disables password authentication for the neighbor.

Task ID

Task ID	Operations
bgp	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to disable MD5 authentication for neighbor 172.20.1.1, preventing it from inheriting the password password1 from session group group1:

```
RP/0/RP0/CPU0:router(config)# router bgp 140
RP/0/RP0/CPU0:router(config-bgp)# session-group group1
RP/0/RP0/CPU0:router(config-bgp-sngrp)# password clear password1
RP/0/RP0/CPU0:router(config-bgp-sngrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 2
RP/0/RP0/CPU0:router(config-bgp-nbr)# use session-group group1
RP/0/RP0/CPU0:router(config-bgp-nbr)# password-disable
```

Related Commands

Command	Description
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
password	Enables MD5 authentication on a TCP connection between two BGP neighbors.
session-group	Creates a session group and enters session group configuration mode.
use	Inherits characteristics from a neighbor group, a session group, or an address family group.

R3.3 Beta Draft—Cisco Confidential Information

rd

To configure a route distinguisher, use the **rd** command in VRF configuration mode. To disable the route distinguisher, use the **no** form of this command.

```
rd {as-number:nn | ip-address:nn | auto}
```

```
no rd {as-number:nn | ip-address:nn | auto}
```

Syntax Description		
<i>as-number:nn</i>	Autonomous system (AS) number of the route distinguisher.	<i>as-number</i>—16-bit AS number <i>nn</i>—32-bit number
<i>ip-address:nn</i>	IP address of the route distinguisher.	<i>ip-address</i>—32-bit IP address <i>nn</i>—16-bit number
auto	Automatically assigns a unique route distinguisher.	

Defaults	No default behavior or values

Command Modes	VRF configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **rd** command to make the prefix unique across multiple VRFs.

Auto assignment of route distinguishers can be done only if a router ID is assigned using the **bgp router-id** command in global configuration mode. The unique router ID is used for automatic route distinguisher generation.

Task ID	Task ID	Operations
	bgp	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to automatically assign a unique route distinguisher to VRF instance vrf-1:

```
RP/0/RP0/CPU0:router(config)# router bgp 1  
RP/0/RP0/CPU0:router(config-bgp)# vrf vrf-1  
RP/0/RP0/CPU0:router(config-bgp-vrf)# rd auto
```

Related Commands

Command	Description
bgp router-id	Configures a fixed router ID for a BGP-speaking router.

R3.3 Beta Draft—Cisco Confidential Information

receive-buffer-size

To set the size of the receive buffers for a Border Gateway Protocol (BGP) neighbor, use the **receive-buffer-size** command in an appropriate configuration mode. To remove the **receive-buffer-size** command from the configuration file and restore the system to its default condition in which the software uses the default size, use the **no** form of this command.

receive-buffer-size *socket-size* [*bgp-size*]

no receive-buffer-size

Syntax Description	<i>socket-size</i>	Size, in bytes, of the receive-side socket buffer. Range is 512 to 131072.
	<i>bgp-size</i>	(Optional) Size, in bytes, of the receive buffer in BGP. Range is 512 to 131072.

Defaults	<i>socket-size</i> : 32,768 bytes <i>bgp-size</i> : 4,032 bytes

Command Modes	Neighbor configuration VRF neighbor configuration Neighbor group configuration Session group configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in VRF neighbor configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **receive-buffer-size** command to increase the buffer size when receiving updates from a neighbor. Using larger buffers can improve convergence time because it allows the software to process a larger number of packets simultaneously. However, allocating larger buffers consumes more memory on the router.

**Note**

Increasing the socket buffer size uses more memory only when more messages are waiting to be processed by the software. In contrast, increasing the BGP buffer size uses extra memory indefinitely.

R3.3 Beta Draft—Cisco Confidential Information

If this command is configured for a neighbor group or session group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

Task ID	Task ID	Operations
	bgp	read, write

Examples

The following example shows how to set the receive buffer sizes for neighbor 172.20.1.1 to be 65,536 bytes for the socket buffer and 8192 bytes for the BGP buffer:

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# receive-buffer-size 65536 8192
```

Related Commands	Command	Description
	neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
	send-buffer-size	Sets the size of the send buffers for a BGP neighbor.
	session-group	Creates a session group and enters session group configuration mode.
	socket receive-buffer-size	Sets the size of the receive buffers for all BGP neighbors.

R3.3 Beta Draft—Cisco Confidential Information

redistribute (BGP)

To redistribute routes from one routing domain into Border Gateway Protocol (BGP), use the **redistribute** command in an appropriate configuration mode. To disable route redistribution, use the **no** form of this command.

Connected

redistribute connected [**metric** *metric-value*] [**route-policy** *route-policy-name*]

no redistribute connected [**metric** *metric-value*] [**route-policy** *route-policy-name*]

Enhanced Interior Gateway Routing Protocol (EIGRP)

redistribute eigrp *process-id* [**match** {**external** | **internal**}] [**metric** *metric-value*] [**route-policy** *route-policy-name*]

no redistribute eigrp *process-id* [**match** {**external** | **internal**}] [**metric** *metric-value*] [**route-policy** *route-policy-name*]

Intermediate System-to-Intermediate System (IS-IS)

redistribute isis *process-id* [**level** {**1** | **1-inter-area** | **2**}] [**metric** *metric-value*] [**route-policy** *route-policy-name*]

no redistribute isis *process-id* [**level** {**1** | **1-inter-area** | **2**}] [**metric** *metric-value*] [**route-policy** *route-policy-name*]

Open Shortest Path First (OSPF)

redistribute ospf *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**route-policy** *route-policy-name*]

no redistribute ospf *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**route-policy** *route-policy-name*]

OSPFv3

redistribute ospfv3 *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**route-policy** *route-policy-name*]

no redistribute ospfv3 *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**route-policy** *route-policy-name*]

Routing Information Protocol

redistribute rip [**metric** *metric-value*] [**route-policy** *route-policy-name*]

no redistribute rip [**metric** *metric-value*] [**route-policy** *route-policy-name*]

R3.3 Beta Draft—Cisco Confidential Information

Static

redistribute static [**metric** *metric-value*] [**route-policy** *route-policy-name*]

no redistribute static [**metric** *metric-value*] [**route-policy** *route-policy-name*]

Syntax	Description
connected	Redistributes connected routes. Connected routes are established automatically when IP is enabled on an interface.
metric <i>metric-value</i>	(Optional) Specifies the metric used for the redistributed route. Range is 0 to 4294967295. Use a value consistent with the destination protocol.
route-policy <i>route-policy-name</i>	(Optional) Specifies a configured routing policy to filter redistributed routes. A route policy is used to filter the importation of routes from this source routing protocol to BGP.
eigrp	Specifies that routes are distributed from EIGRP. You must be in IPv4 unicast or multicast address family configuration mode.
<i>process-id</i>	For the eigrp keyword, an EIGRP instance name from which routes are to be redistributed. For the isis keyword, an IS-IS instance name from which routes are to be redistributed. For the ospf keyword, an OSPF instance name from which routes are to be redistributed. The <i>process-id</i> value takes the form of a string. A decimal number can be entered, but it is stored internally as a string.
match { internal external [1 2] nssa-external [1 2]}	(Optional) Specifies the criteria by which OSPF routes are redistributed into other routing domains. It can be one or more of the following: • internal—Routes that are internal to a specific autonomous system (intra- and inter-area OSPF routes). • external [1 2]—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 external routes. • nssa-external [1 2]—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 not-so-stubby area (NSSA) external routes. For the external and nssa-external options, if a type is not specified, then both Type 1 and Type 2 are assumed.
isis	Specifies that routes are distributed from the IS-IS protocol.
level { 1 1-inter-area 2 }	(Optional) Specifies the IS-IS level from which routes are redistributed. It can be one of the following: • 1—Routes are redistributed from Level 1 routes. • 1-inter-area—Routes are redistributed from Level 1 interarea routes. • 2—Routes are redistributed from Level 2 routes.

R3.3 Beta Draft—Cisco Confidential Information

ospf	Specifies that routes are distributed from the OSPF protocol. You must be in IPv4 unicast or multicast address family configuration mode.
ospfv3	Specifies that routes are distributed from the OSPFv3 protocol. You must be in IPv6 unicast or multicast address family configuration mode.
rip	Specifies that routes are distributed from RIP. You must be in IPv4 unicast or multicast address family configuration mode.
static	Redistributes IP static routes.

Defaults

Route redistribution is disabled.

For IS-IS, the default is to redistribute Level 1 and Level 2 routes.

For OSPF, the default is to redistribute internal, external, and NSSA external routes of Type 1 and Type 2.

For OSPFv3, the default is to redistribute internal, external, and NSSA external routes of Type 1 and Type 2.

By default, the Interior Gateway Protocol (IGP) metric is assigned to the route. For connected and static routes the default metric is 0.

metric *metric-value*: 0

match {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}: If no match is specified, the default is to match all routes.

Command Modes

IPv4 address family configuration

IPv6 address family configuration

VRF IPv4 address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The policy keyword was changed to route-policy . The 1-inter-area and opsfv3 keywords were added.
Release 3.3	The eigrp and rip keywords were added. This command was supported in VRF IPv4 address family configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.



Note

For OSPF you must be in IPv4 unicast or multicast address family configuration mode. For OSPFv3 you must be in IPv6 unicast or multicast address family configuration mode.

R3.3 Beta Draft – Cisco Confidential Information

Each instance of a protocol may be redistributed independently of the others. Changing or removing redistribution for a particular instance does not affect the redistribution capability of other protocols or other instances of the same protocol.

Networks specified using the **network** command are not affected by the **redistribute** command; that is, the routing policy specified in the **network** command takes precedence over the policy specified through the **redistribute** command.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to redistribute IP Version 4 (IPv4) unicast OSPF routes from OSPF instance 110 into BGP:

```
RP/0/RP0/CPU0:router(config)# router bgp 109
RP/0/RP0/CPU0:router(config-bgp)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-af)# redistribute ospf 110
```

Related Commands

Command	Description
network (BGP)	Specifies a local network that the BGP routing process should originate and advertise to its neighbors.

R3.3 Beta Draft—Cisco Confidential Information**remote-as (BGP)**

To create a Border Gateway Protocol (BGP) neighbor and begin the exchange of routing information, use the **remote-as** command in an appropriate configuration mode. To delete the entry for the BGP neighbor, use the **no** form of this command.

remote-as *autonomous-system-number*

no remote-as [*autonomous-system-number*]

Syntax Description

autonomous-system-number Autonomous system to which the neighbor belongs.

Defaults

No BGP neighbors exist.

Command Modes

Neighbor configuration
VRF neighbor configuration
Neighbor group configuration
Session group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF neighbor configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **remote-as** command to create a neighbor and assign it a remote autonomous system number. A neighbor must have a remote autonomous system number before any other commands can be configured for it. Removing the remote autonomous system from a neighbor causes the neighbor to be deleted. You cannot remove the autonomous system number if the neighbor has other configuration.

**Note**

We recommend that you use the **no neighbor** command rather than the **no remote-as** command to delete a neighbor.

A neighbor specified with a remote autonomous system number that matches the autonomous system number specified in the **router bgp** command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered external.

R3.3 Beta Draft—Cisco Confidential Information

Configuration of the **remote-as** command for a neighbor group or session group using the **neighbor-group** command or **session-group** command causes all neighbors using the group to inherit the characteristics configured with the command. Configuring the command directly for the neighbor overrides the value inherited from the group.

In the neighbor configuration submode, configuring use of a session group or neighbor group for which **remote-as** is configured creates a neighbor and assigns it an autonomous system number if the neighbor has not already been created.



Note

Do not combine **remote-as** commands and **no use neighbor-group** commands, or **remote-as** commands and **no use session-group** commands in the same configuration commit.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to assign autonomous system numbers on two neighbors, neighbor 10.0.0.1, (internal) and neighbor 192.168.0.1 (external), setting up a peering session that shares routing information between this router and each of these neighbors:

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.0.0.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 192.168.0.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 2
```

The following example shows how to configure a session group called group2 with an autonomous system number 1. Neighbor 10.0.0.1 is created when it inherits the autonomous system number 1 from session group group2.

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# session-group group2
RP/0/RP0/CPU0:router(config-bgp-sngrp)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-sngrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.0.0.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# use session-group group2
```

Related Commands

Command	Description
neighbor (BGP)	Enters neighbor configuration mode for configuring BGP routing sessions.
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
router bgp	Configures the BGP routing process.
session-group	Creates a session group and enters session group configuration mode.
use	Inherits characteristics from a neighbor group, session group, or address family group.

R3.3 Beta Draft—Cisco Confidential Information

remove-private-as

To remove private autonomous system numbers from autonomous system paths when generating updates to external neighbors, use the **remove-private-as** command in an appropriate configuration mode. To place the router in the default state in which it does not remove private autonomous system numbers, use the **no** form of this command.

remove-private-as [disable]

no remove-private-as

Syntax Description	disable	(Optional) Permits the feature to be disabled from a neighbor group or address family group instead of being inherited.

Defaults	When this command is not specified in the appropriate configuration mode, private autonomous system numbers are not removed from updates sent to external neighbors.

Command Modes	IPv4 address family group configuration IPv6 address family group configuration VPNv4 address family group configuration IPv4 neighbor address family configuration VPNv4 neighbor address family configuration VRF IPv4 neighbor address family configuration IPv4 neighbor group address family configuration IPv6 neighbor group address family configuration VPNv4 neighbor group address family configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in the following configuration modes: • VPNv4 address family group • VPNv4 neighbor address family group • VRF IPv4 neighbor address family • VPNv4 neighbor group address family

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

This feature is available for external BGP (eBGP) neighbors only.

R3.3 Beta Draft—Cisco Confidential Information

When an update is passed to the external neighbor, the software drops any leading autonomous system sequence in the autonomous system path if the sequence contains only private autonomous system numbers and does not contain the autonomous system number of the neighbor.

If this command is used in a BGP confederation, the element following the confederation portion of the autonomous system path, if a sequence, is considered the leading sequence.

The private autonomous system values range from 64512 to 65535.

If this command is configured for a neighbor group or address family group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

Task ID	Task ID	Operations
	bgp	read, write

Examples

The following example shows a configuration that removes the private autonomous system number from the IP Version 4 (IPv4) unicast updates sent to 172.20.1.1:

```
RP/0/RP0/CPU0:router(config)# router bgp 140
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# remove-private-as
```

The following example shows how to disable the remove private autonomous system number feature for neighbor 172.20.1.1, preventing this feature from being automatically inherited from address family group1:

```
RP/0/RP0/CPU0:router(config)# router bgp 140
RP/0/RP0/CPU0:router(config-bgp)# af-group group1 address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-afgrp)# remove-private-as
RP/0/RP0/CPU0:router(config-bgp-afgrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-private-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# use af-group group1
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# remove-private-as disable
```

Related Commands	Command	Description
	af-group	Creates an address family group for BGP neighbors and enters address family group configuration mode.
	neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
	remote-as (BGP)	Allows entries to the BGP neighbor table.

R3.3 Beta Draft—Cisco Confidential Information

retain route-target

To accept received updates with specified route targets, use the **retain route-target** command in VPNv4 address family configuration mode. To disable the retaining of routes tagged with specified route targets, use the **no** form of this command.

retain route-target { **all** | **route-filter** *filter-name* }

no retain route-target { **all** | **route-filter** *filter-name* }

Syntax Description

all	Accepts received updates containing at least one route target.
route-filter <i>filter-name</i>	Accepts received updates accepted by a specified route filter policy.

Defaults

The default is to accept all route targets.

Command Modes

VPNv4 address family configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **retain route-target** command to configure a route reflector (RR) to retain routes tagged with specific route targets (RT).

A provider edge (PE) router is not required to hold all VPNv4 routes. The PE router holds only routes that match the import RT of the VPNs configured on it, but a RR must retain all VPNv4 routes because it may peer with PE routers and different PEs may require different RT-tagged VPNv4 routes.

Configuring an RR to hold only routes that have a defined set of RT communities and configuring some of these RRs to service a different set of VPNs provides scalability to the RRs. A PE can be configured to peer with all RRs that service the VPN routing and forwarding (VRF) instances configured on the PE. When a new VRF is configured with an RT for which the PE does not already hold routes, the PE issues route refresh requests to the RRs and gets the relevant VPN routes.

The **route-filter** *filter-name* keyword and argument takes the policy name that lists the extended communities that a path should have for the RR to retain the path.

Task ID

Task ID	Operations
bgp	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to configure RR to retain all routes with the route filter policy ft-policy-A:

```
RP/0/RP0/CPU0:router(config)# router bgp 140  
RP/0/RP0/CPU0:router(config-bgp)# address-family vpnv4 unicast  
RP/0/RP0/CPU0:router(config-bgp-af)# retain route-target route-filter ft-policy-A
```

Related Commands

Command	Description
import route-target	Configures a VRF import route-target extended community.

R3.3 Beta Draft—Cisco Confidential Information

route-policy (BGP)

To apply a routing policy to updates advertised to or received from a Border Gateway Protocol (BGP) neighbor, use the **route-policy** command in an appropriate configuration mode. To disable applying routing policy to updates, use the **no** form of this command.

route-policy *route-policy-name* {**in** | **out**}

no route-policy *route-policy-name* {**in** | **out**}

Syntax Description

<i>route-policy-name</i>	Name of route policy.
in	Applies policy to inbound routes.
out	Applies policy to outbound routes.

Defaults

No policy is applied.

Command Modes

IPv4 address family group configuration
IPv6 address family group configuration
VPNv4 address family group configuration
IPv4 neighbor address family configuration
VPNv4 neighbor address family configuration
VRF IPv4 neighbor address family configuration
IPv4 neighbor group address family configuration
IPv6 neighbor group address family configuration
VPNv4 neighbor group address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The policy keyword was changed to route-policy .
Release 3.3	This command was supported in the following configuration modes: • VPNv4 address family group • VPNv4 neighbor address family • VRF IPv4 neighbor address family • VPNv4 neighbor group address family

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft – Cisco Confidential Information

Use the **route-policy** command to specify a routing policy for an inbound or outbound route. The policy can be used to filter routes or modify route attributes. The **route-policy** command is used to define a policy.

If the **route-policy** command is configured for a neighbor group or neighbor address family group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to apply the In-Ipv4 policy to inbound IP Version 4 (IPv4) unicast routes from neighbor 172.20.1.1:

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# route-policy In-Ipv4 in
```

Related Commands

Command	Description
af-group	Creates an address family group for BGP neighbors and enters address family group configuration mode.
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
route-policy (RPL)	Defines a route policy and enters route-policy configuration mode.

R3.3 Beta Draft—Cisco Confidential Information

route-reflector-client

To configure the router as a Border Gateway Protocol (BGP) route reflector and configure the specified neighbor as its client, use the **route-reflector-client** command in an appropriate configuration mode. To disable configuring the neighbor as a client, use the **no** form of this command.

route-reflector-client [**disable**]

no route-reflector-client

Syntax Description	disable	(Optional) Allows the configuration inherited from a neighbor group or address family group to be overridden.

Defaults	The neighbor is not treated as a route-reflector client.

Command Modes	IPv4 address family group configuration IPv6 address family group configuration VPNv4 address family group configuration IPv4 neighbor address family configuration VPNv4 neighbor address family configuration IPv4 neighbor group address family configuration IPv6 neighbor group address family configuration VPNv4 neighbor group address family configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in the following configuration modes: • VPNv4 address family group • VPNv4 neighbor address family • VPNv4 neighbor group address family

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

This command is restricted to internal BGP (iBGP) neighbors only.

Use the **route-reflector-client** command to configure the local router as the route reflector and the specified neighbor as one of its clients. All neighbors configured with this command are members of the client group, and the remaining iBGP peers are members of the nonclient group for the local route reflector.

R3.3 Beta Draft—Cisco Confidential Information

By default, all iBGP speakers in an autonomous system must be fully meshed with each other, and neighbors do not readvertise iBGP learned routes to other iBGP neighbors.

With route reflection, all iBGP speakers need not be fully meshed. An iBGP speaker, the route reflector, passes learned iBGP routes to some number of iBGP client neighbors. Learned iBGP routes eliminate the need for each router running BGP to communicate with every other device running BGP in the autonomous system.

The local router is a route reflector as long as it has at least one route reflector client.

If this command is configured for a neighbor group or neighbor address family group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows neighbor at 172.20.1.1 configured as a route reflector client for IP Version 4 (IPv4) unicast routes:

```
RP/0/RP0/CPU0:router(config)# router bgp 140
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 140
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# route-reflector-client
```

The following example disables the route-reflector client for neighbor 172.20.1.1, preventing this feature from being automatically inherited from address family group group1:

```
RP/0/RP0/CPU0:router(config)# router bgp 140
RP/0/RP0/CPU0:router(config-bgp)# af-group group1 address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-afgrp)# route-reflector-client
RP/0/RP0/CPU0:router(config-bgp-afgrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 140
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# use af-group group1
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# route-reflector-client disable
```

Related Commands

Command	Description
af-group	Creates an address family group for BGP neighbors and enters address family group configuration mode.
bgp cluster-id	Configures the cluster ID if the BGP cluster has more than one route reflector.
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.

R3.3 Beta Draft—Cisco Confidential Information

router bgp

To configure the Border Gateway Protocol (BGP) routing process, use the **router bgp** command in global configuration mode. To remove all BGP configurations and terminate the BGP routing process, use the **no** form of this command.

router bgp *autonomous-system-number*

no router bgp

Syntax Description

<i>autonomous-system-number</i>	Number that identifies the autonomous system in which the router resides. Range is 1 to 65535.

Defaults

No BGP routing process is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **router bgp** command to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

Task ID

Task ID	Operations
bgp	read, write
rib	read, write

Examples

The following example shows how to configure a BGP process for autonomous system 120:

```
RP/0/RP0/CPU0:router(config)# router bgp 120
```

R3.3 Beta Draft—Cisco Confidential Information

send-buffer-size

To set the size of the send buffers for a Border Gateway Protocol (BGP) neighbor, use the **send-buffer-size** command in an appropriate configuration mode. To set the size of the send buffers to the default values, use the **no** form of this command.

send-buffer-size *socket-size* [*bgp-size*]

no send-buffer-size

Syntax Description

<i>socket-size</i>	Size, in bytes, of the send-side socket buffer. Range is 4096 to 131072.
<i>bgp-size</i>	(Optional) Size, in bytes, of the BGP process send buffer. Range is 4096 to 131072.

Defaults

socket-size: 4096 bytes

bgp-size: 4096 bytes

Use the **socket send-buffer-size** command to change the defaults.

Command Modes

Neighbor configuration
VRF neighbor configuration
Neighbor group configuration
Session group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF neighbor configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **send-buffer-size** command to increase the buffer size employed when sending updates to a neighbor. Using larger buffers can improve convergence time because the software can process more packets simultaneously. However, allocating larger buffers uses more memory on the router.



Note

Increasing the socket buffer size uses more memory only when more messages are waiting to be processed by the software. In contrast, increasing the BGP buffer size uses more memory indefinitely.

If this command is configured for a neighbor group or session group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	bgp	read, write

Examples

The following example shows how to set the send buffer sizes for neighbor 172.20.1.1 to be 8192 bytes for both the socket buffer and the BGP buffer:

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# send-buffer-size 8192 8192
```

Related Commands

Command	Description
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
receive-buffer-size	Sets the size of the receive buffers for a BGP neighbor.
session-group	Creates a session group and enters session group configuration mode.
socket send-buffer-size	Sets the size of the send buffers for all BGP neighbors.

R3.3 Beta Draft—Cisco Confidential Information

send-community-ebgp

To specify that community attributes should be sent to an external Border Gateway Protocol (eBGP) neighbor, use the **send-community-ebgp** command in an appropriate configuration mode. To disable sending community attributes to an eBGP neighbor, use the **no** form of this command.

send-community-ebgp [disable]

no send-community-ebgp

Syntax Description	disable	(Optional) Allows configuration inherited from a neighbor group or address family group to be overridden.

Defaults	Community attributes are not sent to eBGP neighbors.

Command Modes	IPv4 address family group configuration IPv6 address family group configuration IPv4 neighbor address family configuration VRF IPv4 neighbor address family configuration IPv4 neighbor group address family configuration IPv6 neighbor group address family configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in the VRF IPv4 neighbor address family configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the send-community-ebgp command to control whether community attributes are sent to eBGP neighbors. It cannot be configured for iBGP neighbors. Communities are always sent to iBGP neighbors. If this command is configured for a neighbor group or address family group, all neighbors using the group inherit the configuration. Configuring the command specifically for a neighbor overrides inherited values.

Task ID	Task ID	Operations
	bgp	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to disable the router that sends community attributes to neighbor 172.20.1.1 for IP Version 4 (IPv4) multicast routes:

```
RP/0/RP0/CPU0:router(config)# router bgp 140
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 multicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# send-community-ebgp
```

The following example shows how to disable the delivery of community attributes to neighbor 172.20.1.1, preventing this feature from being inherited from address family group group1:

```
RP/0/RP0/CPU0:router(config)# router bgp 140
RP/0/RP0/CPU0:router(config-bgp)# af-group group1 address-family ipv4 multicast
RP/0/RP0/CPU0:router(config-bgp-afgrp)# send-community-ebgp
RP/0/RP0/CPU0:router(config-bgp-afgrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 multicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# use af-group group1
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# send-community-ebgp disable
```

Related Commands

Command	Description
af-group	Creates an address family group for BGP neighbors and enters address family group configuration mode.
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
send-extended-community-ebgp	Specifies that extended community attributes are sent to eBGP neighbors.

R3.3 Beta Draft—Cisco Confidential Information

send-extended-community-ebgp

To specify that extended community attributes should be sent to external Border Gateway Protocol (eBGP) neighbors, use the **send-extended-community-ebgp** command in an appropriate configuration mode. To disable sending extended community attributes to eBGP neighbors, use the **no** form of this command.

send-extended-community-ebgp [disable]

no send-extended-community-ebgp

Syntax Description	disable	(Optional) Allows configurations inherited from a neighbor group or address family group to be overridden.

Defaults	Extended community attributes are not sent to an eBGP neighbor.

Command Modes	IPv4 address family group configuration IPv6 address family group configuration IPv4 neighbor address family configuration VRF IPv4 neighbor address family configuration IPv4 neighbor group address family configuration IPv6 neighbor group address family configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in the VRF IPv4 neighbor address family configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **send-extended-community-ebgp** command to control whether extended community attributes are sent to eBGP neighbors. It cannot be used for iBGP neighbors. Extended communities are always sent to iBGP neighbors.

If this command is configured for a neighbor group or neighbor address family group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	bgp	read, write

Examples

The following example shows how to configure the router to send extended community attributes to neighbor 172.20.1.1 for IP Version 4 (IPv4) multicast routes:

```
RP/0/RP0/CPU0:router(config)# router bgp 140
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 multicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# send-extended-community-ebgp
```

The following example shows how to disable the delivery of extended community attributes to neighbor 172.20.1.1, preventing this feature from being automatically inherited from address family group group1:

```
RP/0/RP0/CPU0:router(config)# router bgp 140
RP/0/RP0/CPU0:router(config-bgp)# af-group group1 address-family ipv4 multicast
RP/0/RP0/CPU0:router(config-bgp-afgrp)# send-extended-community-ebgp
RP/0/RP0/CPU0:router(config-bgp-afgrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 multicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# use af-group group1
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# send-extended-community-ebgp disable
```

Related Commands

Command	Description
af-group	Creates an address family group for BGP neighbors and enters address family group configuration mode.
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
send-community-ebgp	Specifies that community attributes should be sent to an eBGP neighbor.

R3.3 Beta Draft—Cisco Confidential Information

session-group

To create a session group and enter session group configuration mode, use the **session-group** command in router configuration mode. To remove a session group and delete all configurations associated with it, use the **no** form of this command.

session-group *name*

no session-group *name*

Syntax Description

<i>name</i>	Name of the session group.

Defaults

No session groups are created.

Command Modes

Router configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **session-group** command to create a session group from which neighbors can inherit configuration that is address family-independent. That is, session groups cannot have address family-specific configuration. This command enters the session group configuration mode in which configuration for a session group is entered.

Many commands can be configured in both session group configuration mode and neighbor configuration mode.

Use of session groups saves time and reduces the router configuration size. Because the configuration of a session group can be inherited by any number of neighbors, use of the group can eliminate the need to copy long or complex configurations on each of a large number of neighbors. A neighbor can inherit all configuration from a session group simply by configuring the **use** command. Specific inherited session group configuration commands can be overridden for a specific neighbor by explicitly configuring the command for the specific neighbor.

The **no** form of this command causes all of the configuration for the session group to be removed. You cannot use the **no** form of this command if removing the group would leave one or more neighbors without a configured remote autonomous system number.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	bgp	read, write

Examples

The following example shows a session group called group1 that is used by two neighbors, 10.0.0.1 and 10.0.0.2. Because group1 is a session group, it contains only address family-independent configuration. And because group1 is used by neighbors 10.0.0.1 and 10.0.0.2, they inherit the configuration of the group.

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# session-group group1
RP/0/RP0/CPU0:router(config-bgp-sngrp)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-sngrp)# advertisement-interval 2
RP/0/RP0/CPU0:router(config-bgp-sngrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.0.0.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# use session-group group1
RP/0/RP0/CPU0:router(config-bgp-nbr)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.0.0.2
RP/0/RP0/CPU0:router(config-bgp-nbr)# use session-group group1
```

The following example shows a session group called group1 used by two neighbors, 10.0.0.1 and 10.0.0.2. Because group1 is a session group, it contains only address family-independent configuration. And because group1 is used by neighbors 10.0.0.1 and 10.0.0.2, they inherit the configuration of the group. However, the **password password1** configuration from group1 is overridden for neighbor 10.0.0.2, using the **password-disable** command in the neighbor 10.0.0.2 configuration submode.

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# session-group group1
RP/0/RP0/CPU0:router(config-bgp-sngrp)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-sngrp)# advertisement-interval 2
RP/0/RP0/CPU0:router(config-bgp-sngrp)# password password1
RP/0/RP0/CPU0:router(config-bgp-sngrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.0.0.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# use session-group group1
RP/0/RP0/CPU0:router(config-bgp-nbr)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.0.0.2
RP/0/RP0/CPU0:router(config-bgp-nbr)# use session-group group1
RP/0/RP0/CPU0:router(config-bgp-nbr)# password-disable
```

R3.3 Beta Draft—Cisco Confidential Information

session-open-mode

To establish a Border Gateway Protocol (BGP) session with a specific TCP open mode, use the **session-open-mode** command in an appropriate configuration mode. To end the session, use the **no** form of this command.

session-open-mode { **active-only** | **both** | **passive-only** }

no session-open-mode

Syntax Description

active-only	Ensures that the BGP session can be established only when the request is initiated by the local end (active-open request) and all passive-open requests (from the other end) are rejected by the local BGP.
both	Allows BGP sessions to be established from both incoming or outgoing TCP connection requests, with one being rejected in the event of a request collision.
passive-only	Ensures that the local BGP does not initiate any TCP open requests and the session can be established only when the request comes from the remote end.

Defaults

Session-open-mode is not inherited from the parent.

Command Modes

Neighbor configuration
VRF neighbor configuration
Neighbor group configuration
Session group configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF neighbor configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

BGP, by default, tries to initiate an active TCP connection whenever a new neighbor is configured. A remote neighbor may also initiate the TCP connection before the local BGP can initiate the connection. This initiation of a TCP connection by a remote neighbor is considered a passive-open request and it is accepted by the local BGP. This default behavior can be modified using the **session-open-mode** command.

R3.3 Beta Draft—Cisco Confidential Information

Use the **session-open-mode** command when it may be necessary to pre-configure a neighbor that does not exist. Ensure that BGP does not spend any time actively trying to set up a TCP session with the neighbor. A BGP session does not come up between two neighbors, both of which configure the same nondefault value (**active-only** or **passive-only** keyword) for this command.

Task ID	Task ID	Operations
	bgp	read, write

Examples

The following example shows how to enable a BGP session on router bgp 1:

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# neighbor 45.67.89.01
RP/0/RP0/CPU0:router(config-bgp-nbr)# session-open-mode
```

R3.3 Beta Draft—Cisco Confidential Information

show bgp

To display entries in the Border Gateway Protocol (BGP) routing table, use the **show bgp** command in EXEC mode.

```
show bgp [ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
vpnv4 unicast [rd rd-address] | vrf {vrf-name | all} [ipv4 unicast]] [ip-address [{mask |
/prefix-length} [longer-prefixes | unknown-attributes | bestpath-compare]]
```

Syntax Description

ipv4	(Optional) Specifies IP Version 4 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
all	(Optional) For subaddress families, specifies prefixes for all subaddress families.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
all	(Optional) For address family, specifies prefixes for all address families.
vpnv4 unicast	(Optional) Specifies VPNv4 unicast address families.
rd rd-address	(Optional) Displays routes with a specific route distinguisher.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 unicast	(Optional) For VRF, specifies IPv4 unicast address families.
<i>ip-address</i>	(Optional) Network address, entered to display a particular network in the BGP routing table. If the network address is omitted, then all networks in the BGP routing table are displayed. If the network mask and prefix length is omitted, then the software displays the longest matching prefix for the network address.
<i>mask</i>	(Optional) Network mask of the BGP route to match.
<i>/prefix-length</i>	(Optional) Prefix length of the BGP route to match. A slash (/) must precede the decimal value.
longer-prefixes	(Optional) Displays a route with the specified prefix length and more-specific routes if available. The longer-prefixes keyword is available when the <i>ip-address</i> and <i>mask</i> or <i>/prefix-length</i> arguments are specified.
unknown-attributes	(Optional) Includes unknown, transitive attributes. The unknown-attributes keyword is available when the <i>ip-address</i> and <i>mask</i> or <i>/prefix-length</i> arguments are specified.
bestpath-compare	(Optional) Displays route and best path comparison information. The bestpath-compare keyword is available when the <i>ip-address</i> and <i>mask</i> or <i>/prefix-length</i> arguments are specified.

Defaults

If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

R3.3 Beta Draft—Cisco Confidential Information

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The bestpath-compare keyword was added.
	Release 3.3	The vrf {vrf-name all} and vpnv4 unicast [rd rd-address] keywords and argument were added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.



Note

The **set default-afi** command is used to specify the default address family for the sessions and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

BGP contains a separate routing table for each address family and subaddress family combination that has been configured. The address family and subaddress family options specify the routing table to be examined. If the **all** keyword is specified for an address family or a subaddress family, each matching routing table is examined in turn.

Use the **show bgp ip-address** {mask | /prefix-length} command to display detailed information for a specific route. If the mask and prefix length are omitted, the details of the longest matching prefix for the IP address are displayed.

Use the **show bgp** command to display all routes in the specified BGP routing table. Use the **show bgp ip-address** {mask | /prefix-length} **longer-prefixes** command to display those routes more specific than a particular prefix.

Use the **unknown-attributes** keyword to display details of any transitive attributes associated with a route that are not understood by the local system.

Task ID	Task ID	Operations
	bgp	read

Examples

The following is sample output from the **show bgp** command in EXEC mode:

```
RP/0/RP0/CPU0:router# show bgp
```

```
BGP router identifier 172.20.1.1, local AS number 1820
BGP main routing table version 3
Dampening enabled
BGP scan interval 60 secs
```

R3.3 Beta Draft—Cisco Confidential Information

```

Status codes: s suppressed, d damped, h history, * valid, > best
               i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network        Next Hop        Metric LocPrf Weight Path
* i10.3.0.0/16  172.20.22.1                    0    100    0 1800 1239 ?
*>i             172.20.16.1                    0    100    0 1800 1239 ?
* i10.6.0.0/16  172.20.22.1                    0    100    0 1800 690 568 ?
*>i             172.20.16.1                    0    100    0 1800 690 568 ?
* i10.7.0.0/16  172.20.22.1                    0    100    0 1800 701 35 ?
*>i             172.20.16.1                    0    100    0 1800 701 35 ?
*               192.168.40.24                    0 1878 704 701 35 ?
* i10.8.0.0/16  172.20.22.1                    0    100    0 1800 690 560 ?
*>i             172.20.16.1                    0    100    0 1800 690 560 ?
*               192.168.40.24                    0 1878 704 701 560 ?
* i10.13.0.0/16 172.20.22.1                    0    100    0 1800 690 200 ?
*>i             172.20.16.1                    0    100    0 1800 690 200 ?
*               192.168.40.24                    0 1878 704 701 200 ?
* i10.15.0.0/16 172.20.22.1                    0    100    0 1800 174 ?
*>i             172.20.16.1                    0    100    0 1800 174 ?
* i10.16.0.0/16 172.20.22.1                    0    100    0 1800 701 i
*>i             172.20.16.1                    0    100    0 1800 701 i
*               192.168.40.24                    0 1878 704 701 i

```

Table 1 describes the significant fields shown in the display.

Table 1 *show bgp Field Descriptions*

Field	Description
BGP router identifier	BGP identifier for the local system.
local AS number	Autonomous system number for the local system.
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
Dampening enabled	Dampening is enabled for the routes in this BGP routing table.
BGP scan interval	Interval (in seconds) between BGP scans for the specified address family and subaddress family.
Status codes	Status of the table entry. The status is displayed as a three-character field at the beginning of each line in the table. The first character may be (in order of precedence): S—Path is stale, indicating that a graceful restart is in progress with the peer from which the route was learned. s—Path is more specific than a locally sourced aggregate route and has been suppressed. *—Path is valid. The second character may be (in order of precedence): >—Path is the best path to use for that network. d—Path is dampened. h—Path is a history entry, representing a route that is currently withdrawn, but that is being maintained to preserve dampening information. Such routes should never be marked as valid. The third character may be: i—Path was learned by an internal BGP (iBGP) session.

R3.3 Beta Draft—Cisco Confidential Information

Table 1 *show bgp Field Descriptions (continued)*

Field	Description
Origin codes	Origin of the path. The origin code is displayed at the end of each line in the table. It can be one of the following values: i—Path originated from an Interior Gateway Protocol (IGP) and was sourced by BGP using a network or aggregate-address command. e—Path 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	IP prefix and prefix length for a network.
Next Hop	IP address of the next system that is used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network.
Metric	Value of the interautonomous system metric, otherwise known as the Multi Exit discriminator (MED) metric.
LocPrf	Local preference value. This is used to determine the preferred exit point from the local autonomous system. It is propagated throughout the local autonomous system.
Weight	Path weight. Weight is used in choosing the preferred path to a route. It is not advertised to any neighbor.
Path	Autonomous system path to the destination network. At the end of the path is the path origin code.

The following is sample output from the **show bgp** command with the network specified:

```
RP/0/RP0/CPU0:router# show bgp 11.0.0.0/24
```

```
BGP router table entry for 11.0.0.0/24
```

```
Versions:
```

```
  Process          bRIB/RIB  SendTblVer
  Speaker          2          2
```

```
Paths: (3 available, best #1)
```

```
  Advertised to update-groups (with more than one peer):
```

```
    0.1
```

```
  Advertised to peers (in unique update groups):
```

```
    10.4.101.1
```

```
  Received by speaker 0
```

```
  Local
```

```
    0.0.0.0 from 0.0.0.0 (10.4.0.1)
```

```
      Origin IGP, metric 0, localpref 100, weight 32768, valid, local, best
```

```
  Received by speaker 0
```

```
  2 3 4
```

```
    10.4.101.1 from 10.4.101.1 (10.4.101.1)
```

```
      Origin IGP, localpref 100, valid, external
```

```
  Received by speaker 0
```

```
  Local
```

```
    10.4.101.2 from 10.4.101.2 (10.4.101.2)
```

```
      Origin IGP, localpref 100, valid, internal RP/0/0/CPU0:router#
```

Table 2 describes the significant fields shown in the display.

R3.3 Beta Draft – Cisco Confidential Information

Table 2 *show bgp prefix length Field Descriptions*

Field	Description
BGP router table entry	Network that is being displayed.
Versions	List of the network versions in each BGP process.
Process	Name of the BGP process.
bRIB/RIB	Version of the network for sending to the RIB. You can compare this version with the bRIB/RIB version for the process (at the top of show bgp summary) to verify whether the network has been sent to the RIB.
SendTblVer	Version of the network for advertising to neighbors. This can be compared with the neighbor version to determine whether the network has been advertised to a particular neighbor.
Paths	List of paths for the network (that is, routes to reach the network). The number of paths and the index of the best path are given.
not advertised to any peer	Best path was received with a NO_ADVERTISE community and is not advertised to any neighbor.
not advertised to EBGp peer	Best path was received with a NO_EXPORT community and is not advertised to any eBGP neighbor.
not advertised outside local AS	Best path was received with a LOCAL_AS community and is not advertised to peers outside the local AS.
Advertisements of this net are suppressed by an aggregate	Network is a more-specific prefix of a configured aggregate and has been suppressed. It is not advertised to any neighbors unless they have an unsuppress-map configured.
Advertised to update-groups	List of update-groups to which the net has been advertised. Update-groups that have only one peer are not listed here.
Advertised to peers	List of neighbors to which the net has been advertised to. Neighbors that are in one of the update-groups listed above are not listed separately. Only neighbors that are in unique update-groups are listed.
Received by speaker 0	BGP process where the path originated. This is always “speaker 0.”
AS Path	Autonomous system (AS) path that was received for the path. If the AS path is empty, then “Local” is displayed. This is the case for paths that are locally generated on this router or on a neighboring router within the same AS.
aggregated by	If the path is an aggregate, the router-id of the router that performed the aggregation.
suppressed due to dampening	Path has been suppressed due to the configured path dampening.
history entry	Path is withdrawn, but a copy is kept to store the dampening information.
Received from a RR-client	Path was received from a route reflector client.

R3.3 Beta Draft – Cisco Confidential Information**Table 2** *show bgp prefix length Field Descriptions (continued)*

Field	Description
received-only	If soft reconfiguration inbound is configured, the path was received but dropped by inbound policy, or was accepted and modified. In either event, the received-only value is a copy of the original, unmodified path.
received & used	If soft reconfiguration inbound is configured, the path was received and accepted by inbound policy, but not modified.
stale	Neighbor from which the path was received is down, and the path is kept and marked as stale to support graceful restart.
<nexthop> from <neighbor> (<router-id>)	Nexthop for the path. If the nexthop is known by a mechanism outside BGP (for example, for redistributed paths), then 0.0.0.0 is displayed. After the nexthop, the neighbor from whom the path was received is displayed, along with the neighbor's router-id. If the path was locally generated (for example, an aggregate or redistributed path), then 0.0.0.0 is displayed for the neighbor address.
Origin	IGP: the path originated from an IGP. EGP: the path originated from an EGP. incomplete: the origin of the path is unknown.
metric	MED value of the path.
localpref	Local preference value. This is used to determine the preferred exit point from the local autonomous system. It is propagated throughout the local autonomous system.
weight	Locally assigned weight (if not 0) of the path. Weight is used in choosing the preferred path to a route. It is not advertised to any neighbor.
valid	Path is valid and can be considered in the best path calculation.
redistributed	Path is redistributed through a redistribute command.
aggregated	Path is a locally generated aggregate created due to an aggregate-address command.
local	Path is a local network source due to a network command.
internal	Path was received from an iBGP neighbor.
external	Path was received from an eBGP neighbor.
atomic-aggregate	Path was received with the atomic-aggregate flag set. Some path information has been removed through aggregation.
best	Path is the best path for the network and is used for routing and advertised to peers.
multipath	Path is a multipath and is installed into the RIB along with the best path.
Community	List of communities attached to the path.
Extended community	List of extended communities attached to the path.

R3.3 Beta Draft – Cisco Confidential Information

Table 2 *show bgp prefix length Field Descriptions (continued)*

Field	Description
Originator	Originator of the path within the AS Cluster list if the path is reflected.
AS Cluster list	List of RR clusters the path has passed through if the path is reflected
Dampinfo	Penalty and reuse information if the path is dampened.
penalty	Current penalty for the path.
flapped	Number of times the path has flapped and the time since the first flap.
reuse in	Time until the path is re-used (undampened).
half life	Configured half-life for the path.
suppress value	Penalty at which the path is suppressed.
reuse value	Penalty at which the path is re-used.
Maximum suppress time	Maximum length of time for which the path can be suppressed.

Related Commands

Command	Description
aggregate-address	Creates an aggregate entry in a BGP routing table.
bgp default local-preference	Changes the default local preference value.
network (BGP)	Specifies a local network that the BGP routing process should originate and advertise to its neighbors.
route-policy (BGP)	Applies a routing policy to updates advertised to or received from a BGP neighbor.
set default-afi	Sets the default Address Family Identifier (AFI) for the current session.
set default-safi	Sets the default subaddress Family Identifier (SAFI) for the current session.
show bgp cidr-only	Displays routes with nonnatural netmasks.
show bgp community	Displays routes belonging to the specified communities.
show bgp inconsistent-as	Displays networks with inconsistent origin autonomous system.
show bgp regexp	Displays routes matching an AS path regular expression.
show bgp route-policy	Displays networks that match a route policy.
show bgp summary	Displays the status of all BGP connections.
show bgp truncated-communities	Displays networks with community lists truncated by policy.

R3.3 Beta Draft—Cisco Confidential Information

show bgp advertised

To display advertisements for neighbors or a single neighbor, use the **show bgp advertised** command in EXEC mode.

```
show bgp [{ipv4 | ipv6 | all} {unicast | multicast | all} | [vpn4 unicast] [rd rd-address | vrf
vrf-name] | vrf {vrf-name | all} [ipv4 unicast]] advertised [neighbor ip-address] [summary]
```

Syntax Description	
ipv4	(Optional) Specifies IP Version 4 address prefixes.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
all	(Optional) For address family, specifies prefixes for all address families.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
all	(Optional) For subaddress family, specifies prefixes for all subaddress families.
vpn4 unicast	(Optional) Specifies VPNv4 unicast address families.
rd rd-address	(Optional) Displays routes with a specific route distinguisher.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 unicast	(Optional) For VRF, specifies IPv4 unicast address families.
neighbor	(Optional) Previews advertisements for a single neighbor. If the neighbor keyword is omitted, then the advertisements for all neighbors are displayed.
<i>ip-address</i>	(Optional) IP address of the neighbor.
summary	(Optional) Displays a summary of advertisements.

Defaults If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	The following keywords and arguments were added: vrf {vrf-name all} [ipv4 unicast] [vpn4 unicast] [rd rd-address vrf vrf-name]

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.



Note

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

BGP contains a separate routing table for each address family and subaddress family combination that is configured. The address family and subaddress family options specify the routing table to be examined. If the **all** keyword is specified for the address family or subaddress family, each matching routing table is examined in turn.

Use the **show bgp advertised** command to display the routes that have been advertised to peers or a specific peer. To preview advertisements that would be sent to a peer under a particular policy, even if the corresponding update messages have not been generated yet, use the **show bgp policy** command.



Note

When you issue the **show bgp advertised** command, a route is not displayed in the output unless an advertisement for that route has already been sent (and not withdrawn). If an advertisement for the route has not yet been sent, the route is not displayed.

Use the **summary** keyword to display a summary of the advertised routes. If you do not specify the **summary** keyword, the software displays detailed information about the advertised routes.



Note

The **show bgp advertised** command does not display the application of any outbound policy in the route details it displays. Consequently, this command provides only an indication of whether a particular route has been advertised, rather than details of which attributes were advertised. Use the **show bgp policy sent-advertisements** command to display the attributes that are advertised.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp advertised** command in EXEC mode:

```
RP/0/RP0/CPU0:router# show bgp advertised neighbor 10.0.101.1 summary
```

Network	Next Hop	From
10.0.0.0/16	0.0.0.0	Local
172.16.6.0/24	10.0.101.5	10.0.101.5
172.16.8.0/24	10.0.101.8	10.0.101.8
172.31.0.0/16	0.0.0.0	Local Aggregate

Table 3 describes the significant fields shown in the display.

R3.3 Beta Draft—Cisco Confidential Information

Table 3 *show bgp advertised neighbor summary Field Descriptions*

Field	Description
Network	IP prefix and prefix length for a network.
Next Hop	IP address of the next system that is used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network.
From	IP address of the peer that advertised this route.
Local	Indicates the route originated on the local system.
Local Aggregate	Indicates the route is an aggregate created on the local system.
Advertised to	Indicates the peer to which this entry was advertised. This field is used in the output when displaying a summary of the advertisements to all neighbors.

The following is sample output from the **show bgp advertised** command for detailed advertisement information:

```
RP/0/RP0/CPU0:router# show bgp advertised neighbor 172.72.77.1

172.16.0.0/24 is advertised to 172.72.77.1
  Path info:
    neighbor: Local          neighbor router id: 172.74.84.1
    valid redistributed best
  Attributes after inbound policy was applied:
    next hop: 0.0.0.0
    MET ORG AS
    origin: incomplete metric: 0
    aspath:
10.52.0.0/16 is advertised to 172.72.77.1
  Path info:
    neighbor: Local Aggregate neighbor router id: 172.74.84.1
    valid aggregated best
  Attributes after inbound policy was applied:
    next hop: 0.0.0.0
    ORG AGG ATOM
    origin: IGP aggregator: 172.74.84.1 (1)
    aspath:
```

Table 4 describes the significant fields shown in the display.

Table 4 *show bgp advertised neighbor Field Descriptions*

Field	Description
is advertised to	IP address of the peer to which this route has been advertised. If the route has been advertised to multiple peers, the information is shown separately for each peer.
neighbor	IP address of the peer that advertised this route, or one of the following: Local—Route originated on the local system. Local Aggregate—Route is an aggregate created on the local system.

R3.3 Beta Draft—Cisco Confidential Information

Table 4 *show bgp advertised neighbor Field Descriptions (continued)*

Field	Description
neighbor router id	BGP identifier for the peer, or the local system if the route originated on the local system.
Not advertised to any peer	Indicates the no-advertise well-known community is associated with this route. Routes with this community are not advertised to any BGP peers.
Not advertised to any EBGp peer	Indicates the no-export well-known community is associated with this route. Routes with this community are not advertised to external BGP peers, even if those external peers are part of the same confederation as the local router.
Not advertised outside the local AS	Indicates the local-AS well-known community is associated with this route. Routes with this community value are not advertised outside the local autonomous system or confederation boundary.
(Received from a RR-client)	Path was received from a route reflector client.
(received-only)	This path is not used for routing purposes. It is used to support soft reconfiguration, and records the path attributes before inbound policy was applied to a path received from a peer. A path marked “received-only” indicates that either the path was dropped by inbound policy, or the path information was modified by inbound policy and a separate copy of the modified path is used for routing.
(received & used)	Indicates that the path is used both for soft reconfiguration and routing purposes. A path marked “received and used,” implies the path information was not modified by inbound policy.
valid	Path is valid.
redistributed	Path is locally sourced through redistribution.
aggregated	Path is locally sourced through aggregation.
local	Path is locally sourced through the network command.
confed	Path was received from a confederation peer.
best	Path is selected as best.
multipath	Path is one of multiple paths selected for load-sharing purposes.
dampinfo	Indicates dampening information: Penalty—Current penalty for this path. Flapped—Number of times the route has flapped. In—Time (hours:minutes:seconds) since the router noticed the first flap. Reuse in—Time (hours:minutes:seconds) after which the path is made available. This field is displayed only if the path is currently suppressed.

R3.3 Beta Draft—Cisco Confidential Information

Table 4 *show bgp advertised neighbor Field Descriptions (continued)*

Field	Description
Attributes after inbound policy was applied	Displays attributes associated with the received route, after any inbound policy has been applied. AGG—Aggregator attribute is present. AS—AS path attribute is present. ATOM—Atomic aggregate attribute is present. COMM—Communities attribute is present. EXTCOMM—Extended communities attribute is present. LOCAL—Local preference attribute is present. MET—Multi Exit Discriminator (MED) attribute is present. next hop—IP address of the next system used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network. ORG—Origin attribute is present.
origin	Origin of the path: IGP—Path originated from an Interior Gateway Protocol (IGP) and was sourced by BGP using a network or aggregate-address command. EGP—Path originated from an Exterior Gateway Protocol. incomplete—Origin of the path is not clear. For example, a route that is redistributed into BGP from an IGP.
neighbor as	First autonomous system (AS) number in the AS path.
aggregator	Indicates that the path was received with the aggregator attribute. The autonomous system number and router-id of the system that performed the aggregation are shown.
metric	Value of the interautonomous system metric, otherwise known as the MED metric.
localpref	Local preference value. This is used to determine the preferred exit point from the local autonomous system. It is propagated throughout the local autonomous system
aspath	AS path associated with the route.
community	Community attributes associated with the path. Community values are displayed in AA:NN format, except for the following well-known communities: Local-AS—Community with value 4294901812. Routes with this community value are not advertised outside the local autonomous system or confederation boundary. no-advertise—Community with value 4294901813. Routes with this community value are not advertised to any BGP peers. no-export—Community with value 4294901814. Routes with this community are not advertised to external BGP peers, even if those peers are in the same confederation with the local router.

R3.3 Beta Draft—Cisco Confidential Information

Table 4 *show bgp advertised neighbor Field Descriptions (continued)*

Field	Description
Extended community	Extended community attributes associated with the path. For known extended community types, the following codes may be displayed: RT—Route target community SoO—Site of Origin community LB—Link Bandwidth community
Originator	Router ID of the originating router when route reflection is used.
Cluster lists	Router ID or cluster ID of all route reflectors through which the route has passed.

Related Commands

Command	Description
set default-afi	Sets the default Address Family Identifier (AFI) for the current session.
set default-safi	Sets the default subaddress Family Identifier (SAFI) for the current session.
route-policy (BGP)	Applies a route policy to incoming and outgoing routes.
rd	Filters routes using a prefix list.
show bgp policy	Displays information about BGP advertisements under a proposed policy.
show bgp policy sent-advertisements	Previews advertisements to peers, including details of advertised attributes.

R3.3 Beta Draft—Cisco Confidential Information

show bgp af-group

To display information about Border Gateway Protocol (BGP) configuration for address family groups, use the **show bgp af-group** command in EXEC mode.

```
show bgp af-group group-name {configuration [defaults] [nvgen] | inheritance | users}
```

Syntax Description	
<i>group-name</i>	Name of the address family group to display.
configuration	(Optional) Displays the effective configuration for the af-group, including any settings that have been inherited from af-groups used by this af-group.
defaults	(Optional) Displays all configuration settings, including any default settings.
nvgen	(Optional) Displays output in the format of show running-config output. Note If the defaults keyword is also specified, the output is not suitable for cutting and pasting into a configuration session.
inheritance	Displays the af-groups from which this af-group inherits configuration settings.
users	Displays the neighbors, neighbor groups, and af-groups that inherit configuration from this af-group.

Defaults No default behavior or value

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show bgp af-group** command with the *group-name* **configuration** argument and keyword to display the effective configuration of an af-group, taking into account any configuration that may be inherited from other af-groups through the **use af-group** command. The source of each command is shown.

If the **defaults** keyword is specified, all configuration for the af-group, including default values, is shown. Default configuration is identified in the show output. Use the **nvgen** keyword to display configuration formatted in the style of the **show running-config** command. This output is suitable for cutting and pasting into configuration sessions.

R3.3 Beta Draft—Cisco Confidential Information

Use the **show bgp af-group** command with the *group-name* **inheritance** argument and keyword to display the address family groups from which the specified af-group inherits configuration.

Use the **show bgp af-group** command with the *group-name* **users** argument and keyword to display the neighbors, neighbor groups, and af-groups that inherit configuration from the specified af-group.

Task ID

Task ID Operations

bgp	read

Examples

The following af-group configuration is used in the examples:

```
af-group group3 address-family ipv4 unicast
remove-private-AS
soft-reconfiguration inbound
!
af-group group1 address-family ipv4 unicast
use af-group group2
maximum-prefix 2500 75 warning-only
default-originate
soft-reconfiguration inbound disable
!
af-group group2 address-family ipv4 unicast
use af-group group3
send-community-ebgp
send-extended-community-ebgp
capability orf prefix-list both
```

The following is sample output from the **show bgp af-group** command with the **configuration** keyword in EXEC mode. The source of each command is shown in the right column. For example, **default-originate** is configured directly on **af-group group1**, and the **remove-private-AS** command is inherited from af-group group2, which in turn inherits it from af-group group3.

```
RP/0/RP0/CPU0:router# show bgp af-group group1 configuration

af-group group1 address-family ipv4 unicast
  capability orf prefix-list both          [a:group2]
  default-originate                        []
  maximum-prefix 2500 75 warning-only      []
  remove-private-AS                        [a:group2 a:group3]
  send-community                           [a:group2]
  send-extended-community                  [a:group2]
```

The following is sample output from the **show bgp af-group** command with the **users** keyword:

```
RP/0/RP0/CPU0:router# show bgp af-group group2 users

IPv4 Unicast: a:group1
```

The following is sample output from the **show bgp af-group** command with the **inheritance** keyword. This example shows that the specified af-group group1 directly uses the group2 af-group, which in turn uses the group3 af-group:

```
RP/0/RP0/CPU0:router# show bgp af-group group1 inheritance

IPv4 Unicast: a:group2 a:group3
```

Table 5 describes the significant fields shown in the display.

R3.3 Beta Draft – Cisco Confidential Information

Table 5 *show bgp af-group Field Descriptions*

Field	Description
[]	Configures the command directly on the specified address family group.
a:	Indicates the name that follows is an address family group.
n:	Indicates the name that follows is a neighbor group.
[dflt]	Indicates the setting is not explicitly configured or inherited, and the default value for the setting is used. This field may be shown when the defaults keyword is specified.
<not set>	Indicates that the configuration is disabled by default. This field may be shown when the defaults keyword is specified.

Related Commands

Command	Description
af-group	Configures a BGP address family group.
show bgp neighbors	Displays information about BGP neighbors, including configuration inherited from neighbor groups, session groups, and address family groups.
show bgp neighbor-group	Displays information about configuration for neighbor groups.
use af-group	Configures an af-group to inherit the configuration of a specified af-group.

R3.3 Beta Draft—Cisco Confidential Information

show bgp attribute-key

To display all existing attribute keys, use the **show bgp attribute-key** command in EXEC mode.

```
show bgp [ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all}]
attribute-key [count-only]
```

Syntax Description

ipv4	(Optional) Specifies IP Version 4 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
all	(Optional) For subaddress families, specifies prefixes for all subaddress families.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
all	(Optional) For address family, specifies prefixes for all address families.
count-only	(Optional) Displays the number of prefixes or paths.

Defaults

If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

**Note**

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

Task ID

Task ID	Operations
bgp	read

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following is sample output from the **show bgp attribute-key** command in EXEC mode:

```
RP/0/RP0/CPU0:router# show bgp all all attribute-key

Address Family: IPv4 Unicast
=====

BGP router identifier 10.0.0.1, local AS number 1
BGP generic scan interval 60 secs
BGP main routing table version 109
BGP scan interval 60 secs
Status codes: s suppressed, d damped, h history, * valid, > best
                i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          AttrKey
*> 1.1.0.0/16        0.0.0.0            0x00000002
*> 10.0.0.0/16       0.0.0.0            0x00000002
*> 12.21.0.0/16      0.0.0.0            0x00000002
*> 194.3.192.1/32    10.0.101.1         0x00000009
*> 194.3.192.2/32    10.0.101.1         0x00000009
*> 194.3.192.3/32    10.0.101.1         0x00000009
*> 194.3.192.4/32    10.0.101.1         0x00000009
*> 194.3.192.5/32    10.0.101.1         0x00000009

Processed 8 prefixes, 8 paths

Address Family: IPv4 Multicast
=====

BGP router identifier 10.0.0.1, local AS number 1
BGP generic scan interval 60 secs
BGP main routing table version 15
BGP scan interval 60 secs
Status codes: s suppressed, d damped, h history, * valid, > best
                i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          AttrKey
*> 194.3.193.2/32    10.0.101.1         0x00000009
*> 194.3.193.3/32    10.0.101.1         0x00000009

Processed 2 prefixes, 2 paths

Address Family: IPv6 Unicast
=====

BGP router identifier 10.0.0.1, local AS number 1
BGP generic scan interval 60 secs
BGP main routing table version 19
BGP scan interval 60 secs
Status codes: s suppressed, d damped, h history, * valid, > best
                i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          AttrKey
*> 2222::1111/128    2222::2            0x00000009
*> 2222::1112/128    2222::2            0x00000009

Processed 2 prefixes, 2 paths
```

Table 6 describes the significant fields shown in the display.

R3.3 Beta Draft—Cisco Confidential Information

Table 6 *show bgp attribute-key Field Descriptions*

Field	Description
BGP router identifier	BGP identifier for the local system.
local AS number	Autonomous system number for the local system.
BGP generic scan interval	Interval (in seconds) between scans for garbage collection across all address family-independent tables.
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
BGP scan interval	Interval (in seconds) between scans.
Status codes	Status of the table entry. The status is displayed as a three-character field at the beginning of each line in the table. The first character may be (in order of precedence): S—Path is stale, indicating that a graceful restart is in progress with the peer from which the route was learned. s—Path is more specific than a locally sourced aggregate route and has been suppressed. *—Path is valid. The second character may be (in order of precedence): >—Path is the best path to use for that network. d—Path is dampened. h—Path is a history entry, representing a route that is currently withdrawn, but that is being maintained to preserve dampening information. Such routes should never be marked as valid. The third character may be: i—Path was learned by an internal BGP (iBGP) session.
Origin codes	Origin of the path. The origin code is displayed at the end of each line in the table. It can be one of the following values: i—Path originated from an Interior Gateway Protocol (IGP) and was sourced by BGP using a network or aggregate-address 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	IP prefix and prefix length for a network.
Next Hop	IP address of the next system that is used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network.
AttrKey	Key associated with the route attribute.
Processed <i>n</i> prefixes, <i>n</i> paths	Number of prefixes and number of paths processed for the table.

R3.3 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	set default-afi	Sets the default Address Family Identifier (AFI) for the current session.
	set default-safi	Sets the default Subaddress Family Identifier (SAFI) for the current session.

R3.3 Beta Draft—Cisco Confidential Information

show bgp cidr-only

To display routes with nonnatural network masks, also known as classless interdomain routing (CIDR) routes, use the **show bgp cidr-only** command in EXEC mode.

```
show bgp [ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
ip-address {mask | /prefix-length} longer-prefixes | [vpnv4 unicast] [rd rd-address] | vrf
{vrf-name | all} [ipv4 unicast]] cidr-only [count-only]
```

Syntax Description

ipv4	(Optional) Specifies the IP Version 4 address family.
unicast	(Optional) Specifies the unicast address family.
multicast	(Optional) Specifies the multicast address family.
all	(Optional) For subaddress family, specifies all subaddress families.
ipv6	(Optional) Specifies the IP Version 6 address family.
all	(Optional) For address family, specifies all address families.
<i>ip-address</i>	(Optional) Show flap statistics for network address only.
<i>mask</i>	(Optional) Network mask applied to the <i>ip-address</i> argument.
<i>/prefix-length</i>	(Optional) Length of the IP address prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash (/) must precede the decimal value.
longer-prefixes	(Optional) Displays flap statistics for the specified prefix and more-specific prefixes. The longer-prefixes keyword is available when <i>ip-address</i> and <i>mask</i> or <i>/prefix-length</i> arguments are specified.
vpnv4 unicast	(Optional) Specifies VPNv4 unicast address families.
rd rd-address	(Optional) Displays routes with a specific route distinguisher.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 unicast	(Optional) For VRF, specifies IPv4 unicast address families.
count-only	(Optional) Displays the number of prefixes or paths.

Defaults

If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used. This command is applicable only for IPv4 prefixes. If the default address family is not IPv4, then the **ipv4** keyword must be used.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Release	Modification
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The count-only keyword was added.
Release 3.3	The following keywords and arguments were added: vrf {vrf-name all} [ipv4 unicast] [vpn4 unicast] [rd rd-address]

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.



Note

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

Border Gateway Protocol (BGP) contains a separate routing table for each address family and subaddress family combination that has been configured. The address family and subaddress family options specify the routing table to be examined. If the **all** keyword is specified for subaddress family, all subaddress family routing tables are examined.

The **show bgp cidr-only** command applies only for IPv4 prefixes. If the **ipv4** keyword is not specified and the default address family is not IPv4, the command is not available.

Use the **show bgp cidr-only** command to display CIDR routes. Routes that have their correct class (class A, B, or C) prefix length are not displayed.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp cidr-only** command in EXEC mode:

```
RP/0/RP0/CPU0:router# show bgp cidr-only

BGP router identifier 172.20.1.1, local AS number 1820
BGP main routing table version 2589
Dampening enabled
BGP scan interval 60 secs
Status codes: s suppressed, d damped, h history, * valid, > best
               i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network        Next Hop        Metric      LocPrf   Weight    Path
*> 192.0.0.0/8  192.168.72.24      0           1878     ?
*> 192.168.0.0/16 192.168.72.30      0           108      ?
```

Table 7 describes the significant fields shown in the display.

R3.3 Beta Draft—Cisco Confidential Information

Table 7 *show bgp cidr-only Field Descriptions*

Field	Description
BGP router identifier	BGP identifier for the local system.
local AS number	Autonomous system number for the local system.
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
Dampening enabled	Displayed if dampening is enabled for the routes in this BGP routing table.
BGP scan interval	Interval (in seconds) between scans of the BGP table specified by the address family and subaddress family.
Status codes	Status of the table entry. The status is displayed as a three-character field at the beginning of each line in the table. The first character may be (in order of precedence): S—Path is stale, indicating that a graceful restart is in progress with the peer from which the route was learned. s—Path is more specific than a locally sourced aggregate route and has been suppressed. *—Path is valid. The second character may be (in order of precedence): >—Path is the best path to use for that network. d—Path is dampened. h—Path is a history entry, representing a route that is currently withdrawn, but that is being maintained to preserve dampening information. Such routes should never be marked as valid. The third character may be: i—Path was learned by an internal BGP (iBGP) session.
Origin codes	Origin of the path. The origin code is displayed at the end of each line in the table. It can be one of the following values: i—Path originated from an Interior Gateway Protocol (IGP) and was sourced by BGP using a network or aggregate-address 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	IP prefix and prefix length for a network.
Next Hop	IP address of the next system that is used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network.
Metric	Value of the interautonomous system metric, otherwise known as the Multi Exit Discriminator (MED) metric.

R3.3 Beta Draft—Cisco Confidential Information

Table 7 *show bgp cidr-only Field Descriptions (continued)*

Field	Description
LocPrf	Local preference value. This is used to determine the preferred exit point from the local autonomous system. It is propagated throughout the local autonomous system.
Weight	Path weight. Weight is used in choosing the preferred path to a route. It is not advertised to any neighbor.
Path	Autonomous system path to the destination network. At the end of the path is the origin code for the path.

Related Commands

Command	Description
route-policy (BGP)	Applies a routing policy to updates advertised to or received from a BGP neighbor
set default-afi	Sets the default Address Family Identifier (AFI) for the current session.
set default-safi	Sets the default Subaddress Family Identifier (SAFI) for the current session.
show bgp	Displays BGP routes.

R3.3 Beta Draft—Cisco Confidential Information

show bgp community

To display routes that have the specified Border Gateway Protocol (BGP) communities, use the **show bgp community** command in EXEC mode.

```
show bgp [ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
[vpn4 unicast] [rd rd-address] | vrf {vrf-name | all} [ipv4 unicast]] community
community-list [exact-match] [count-only]
```

Syntax Description

ipv4	(Optional) Specifies IP Version 4 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
all	(Optional) For subaddress families, specifies prefixes for all subaddress families.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
all	(Optional) For address family, specifies prefixes for all address families.
vpn4 unicast	(Optional) Specifies VPNv4 unicast address families.
rd rd-address	(Optional) Displays routes with a specific route distinguisher.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 unicast	(Optional) For VRF, specifies IPv4 unicast address families.
community	Specifies that only routes with communities specified by <i>community-list</i> is displayed.
<i>community-list</i>	Between one and seven communities. Each community can be a number in the range from 1 to 4294967295, a community specified in AA:NN format, or one of the following well-known communities: • local-AS—Well-known community with value 4294901812. Routes with this community value are not advertised outside the local autonomous system or confederation boundary. • no-advertise—Well-known community with value 4294901813. Routes with this community value are not advertised to any BGP peers. • no-export—Well-known community with value 4294901814. Routes with this community are not advertised to external BGP peers, even if those peers are in the same confederation as the local router. • internet—Well-known community whose value is not defined in BGP RFC. IOS XR BGP uses a value of 0 for the internet community. Routes with this community are advertised to all peers without any restrictions. For the AA:NN format: • AA—Range is 0 to 65535. • NN—Range is 1 to 4294967295. Up to seven community numbers can be specified.

R3.3 Beta Draft—Cisco Confidential Information

exact-match	(Optional) Displays those routes that have communities exactly matching the specified communities.
count-only	(Optional) Displays the number of prefixes or paths.

Defaults

If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The count-only keyword was added.
Release 3.3	The following keywords and arguments were added: vrf {<i>vrf-name</i> all} [ipv4 unicast] [vpn4 unicast] [rd rd-address]

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.



Note

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

BGP contains a separate routing table for each configured address family and subaddress family combination. The address family and subaddress family options specify the routing table to be examined. If the **all** keyword is specified for the address family or the subaddress family, each matching routing table is examined in turn.

If more than seven communities are required, it is necessary to configure a route policy and use the [show bgp route-policy](#) command.

Use the **exact-match** keyword to display only those routes with a set of communities exactly matching the list of specified communities. If you omit the **exact-match** keyword, those routes containing at least the specified communities are displayed.

Task ID

Task ID	Operations
bgp	read

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following is sample output from the **show bgp community** command in EXEC mode:

```
RP/0/RP0/CPU0:router# show bgp community 1820:1 exact-match

BGP router identifier 172.20.1.1, local AS number 1820
BGP main routing table version 55
Dampening enabled
BGP scan interval 60 secs
Status codes: s suppressed, d damped, h history, * valid, > best
                i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*  10.13.0.0/16      192.168.40.24              0 1878 704 701 200 ?
*  10.16.0.0/16      192.168.40.24              0 1878 704 701 i
```

Table 8 describes the significant fields shown in the display.

Table 8 *show bgp community Field Descriptions*

Field	Description
BGP router identifier	BGP identifier for the local system.
local AS number	Autonomous system number for the local system.
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
Dampening enabled	Displayed if dampening is enabled for the routes in this BGP routing table.
BGP scan interval	Interval (in seconds) between scans of the BGP table specified by the address family and subaddress family.
Status codes	Status of the table entry. The status is displayed as a three character field at the beginning of each line in the table. The first character may be (in order of precedence): S—Path is stale, indicating that a graceful restart is in progress with the peer from which the route was learned. s—Path is more specific than a locally sourced aggregate route and has been suppressed. *—Path is valid. The second character may be (in order of precedence): >—Path is the best path to use for that network. d—Path is dampened. h—Path is a history entry, representing a route that is currently withdrawn, but that is being maintained to preserve dampening information. Such routes should never be marked as valid. The third character may be: i—Path was learned by an internal BGP (iBGP) session.

R3.3 Beta Draft—Cisco Confidential Information**Table 8** *show bgp community Field Descriptions (continued)*

Field	Description
Origin codes	Origin of the path. The origin code is displayed at the end of each line in the table. It can be one of the following values: i—Path originated from an Interior Gateway Protocol (IGP) and was advertised with a network or aggregate-address command. e—Path 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	IP prefix and prefix length for a network.
Next Hop	IP address of the next system that is used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network.
Metric	Value of the interautonomous system metric, otherwise known as the Multi Exit Discriminator (MED) metric.
LocPrf	Local preference value. This is used to determine the preferred exit point from the local autonomous system. It is propagated throughout the local autonomous system.
Weight	Path weight. Weight is used in choosing the preferred path to a route. It is not advertised to any neighbor.
Path	Autonomous system path to the destination network. At the end of the path is the the origin code for the path.

Related Commands

Command	Description
aggregate-address	Creates an aggregate entry in a BGP routing table.
network (BGP)	Specifies a local network that the BGP routing process should originate and advertise to its neighbors.
route-policy (BGP)	Applies a routing policy to updates advertised to or received from a BGP neighbor
set default-afi	Sets the default Address Family Identifier (AFI) for the current session.
set default-safi	Sets the default Subaddress Family Identifier (SAFI) for the current session.
show bgp	Displays BGP routes.

R3.3 Beta Draft—Cisco Confidential Information

show bgp convergence

To display whether a specific address family has reached convergence, use the **show bgp convergence** command in EXEC mode.

```
show bgp [ipv4 { unicast | multicast | all } | ipv6 { unicast | all } | all { unicast | multicast | all } |  
vpn4 unicast | vrf { vrf-name | all } [ipv4 unicast]] convergence
```

Syntax Description	
ipv4	(Optional) Specifies the IP Version 4 address family.
unicast	(Optional) Specifies the unicast address family.
multicast	(Optional) Specifies the multicast address family.
all	(Optional) For subaddress family, specifies all subaddress families.
ipv6	(Optional) Specifies the IP Version 6 address family.
all	(Optional) For address family, specifies all address families.
vpn4 unicast	(Optional) Specifies VPNv4 unicast address families.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 unicast	(Optional) For VRF, specifies IPv4 unicast address families.

Defaults If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	The following keywords and arguments were added: vrf { vrf-name all } [ipv4 unicast] vpn4 unicast

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information



Note

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

Border Gateway Protocol (BGP) contains a separate routing table for each configured address family and subaddress family combination. The address family and subaddress family options specify the routing table to be examined. If the **all** keyword is specified for the address family or subaddress family, each matching routing table is examined in turn.

Use the **show bgp convergence** command to see if there is any pending work for BGP to perform. The software checks the following conditions to determine whether the specified address family has converged. If all the conditions are true, the address family is considered converged.

- All received updates have been processed and best routes selected.
- All selected routes have been installed in the global Routing Information Base (RIB).
- All selected routes have been advertised to peers, including any peers that are not established (unless those peers have been administratively shut down). See the **shutdown (BGP)** command for more information about administrative shutdown.

While testing that all selected routes have been advertised to peers, the **show bgp convergence** command checks the size of the write queue for each neighbor. Because this queue is shared by all address families, there is a small possibility that the command indicates the address family has not converged when, in fact, it has converged. This could happen if the neighbor write queue contained messages from some other address family.

If the specified address family has not converged, the **show bgp convergence** command output does not indicate the amount of work that is pending. To display this information, use the **show bgp summary** command.

Task ID	Task ID	Operations
	bgp	read

Examples

The following shows the result of using the **show bgp convergence** command for an address family that has converged:

```
RP/0/RP0/CPU0:router# show bgp convergence
```

```
Converged.
All received routes in RIB, all neighbors updated.
All neighbors have empty write queues.
```

The following shows the result of using the **show bgp convergence** command for an address family that has not converged:

```
RP/0/RP0/CPU0:router# show bgp convergence
```

```
Not converged.
Received routes may not be entered in RIB.
One or more neighbors may need updating.
```

R3.3 Beta Draft – Cisco Confidential Information

Table 9 describes the significant fields shown in the display.

Table 9 *show bgp convergence Field Descriptions*

Field	Description
Converged/Not converged	Specifies whether or not all routes have been installed in the RIB and updates have been generated and sent to all neighbors.
[All] Received routes...	For convergence, all routes must have been installed into the RIB and all updates must have been generated. For non-convergence, some routes may not be installed in the RIB, or some routes that have been withdrawn have not yet been removed from the RIB, or some routes that are up to date in the RIB have not been advertised to all neighbors.
[All One or more] neighbors...	Specifies the status of neighbor updating.

Related Commands

Command	Description
set default-afi	Sets the default Address Family Identifier (AFI) for the current session.
set default-safi	Sets the default Subaddress Family Identifier (SAFI) for the current session.
show bgp convergence	Displays whether a specific address family has reached convergence.
show bgp summary	Displays the status of BGP peer connections.
shutdown (BGP)	Disables a neighbor without removing all of its configuration.

R3.3 Beta Draft—Cisco Confidential Information

show bgp count-only

To display a count of the number of prefixes and paths in the Border Gateway Protocol (BGP) table that match the specified (or none) filter instead of displaying the details of each of the individual paths in the table, use the **show bgp count-only** command in EXEC mode.

```
show bgp [ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
ip-address {mask | /prefix-length} longer-prefixes | [vpnv4 unicast] [rd rd-address | vrf
{vrf-name | all} [ipv4 unicast]] [cidr-only | route-policy route-policy-name |
truncated-communities | community community-list [exact-match] | attribute-key]
count-only
```

Syntax	Description
ipv4	(Optional) Specifies the IP Version 4 address family.
unicast	(Optional) Specifies the unicast address family.
multicast	(Optional) Specifies the multicast address family.
all	(Optional) For subaddress family, specifies all subaddress families.
ipv6	(Optional) Specifies the IP Version 6 address family.
all	(Optional) For address family, specifies all address families.
<i>ip-address</i>	(Optional) Show flap statistics for network address only.
<i>mask</i>	(Optional) Network mask applied to the <i>ip-address</i> argument.
<i>/prefix-length</i>	(Optional) Length of the IP address prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash (/) must precede the decimal value.
longer-prefixes	(Optional) Displays flap statistics for the specified prefix and more-specific prefixes. The longer-prefixes keyword is available when <i>ip-address</i> and <i>mask</i> or <i>/prefix-length</i> arguments are specified.
vpnv4 unicast	(Optional) Specifies VPNv4 unicast address families.
rd rd-address	(Optional) Displays routes with a specific route distinguisher.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 unicast	(Optional) For VRF, specifies IPv4 unicast address families.
cidr-only	(Optional) Displays only routes whose prefix length does not match the classful prefix length for that network. The cidr-only keyword can be specified only if the address family is IPv4.
route-policy	(Optional) Displays advertisements for an output route policy.
<i>route-policy-name</i>	(Optional) Name of the route policy.
truncated-communities	(Optional) Displays networks with community lists truncated by policy
community	(Optional) Specifies that only routes with communities specified by <i>community-list</i> is displayed.

R3.3 Beta Draft—Cisco Confidential Information

<i>community-list</i>	(Optional) Between one and seven communities. Each community can be a number in the range from 1 to 4294967295, a community specified in AA:NN format, or one of the following well-known communities: – local-AS—Well-known community with the value 4294901812. Routes with this community value are not advertised outside the local autonomous system or confederation boundary. – no-advertise—Well-known community with the value 4294901813. Routes with this community value are not advertised to any BGP peers. – no-export—Well-known community with the value 4294901814. Routes with this community are not advertised to external BGP peers, even if those peers are in the same confederation as the local router. For the AA:NN format: • AA—Range is 0 to 65535. • NN—Range is 1 to 4294967295. Up to seven community numbers can be specified.
exact-match	(Optional) Displays those routes that have communities exactly matching the specified communities.
attribute-key	(Optional) Displays networks with the associated attribute key indexes. This keyword is not supported when vpn4 unicast and vrf are selected.

Defaults

If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used. This command is applicable only for IPv4 prefixes. If the default address family is not IPv4, then the **ipv4** keyword must be used.

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.3	The following keywords and arguments were added: • vrf {vrf-name all} [ipv4 unicast] • [vpn4 unicast] [rd rd-address]

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information



Note

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

Use the **show bgp count-only** command to obtain a count of the number of entries in a BGP table.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp count-only** command in EXEC mode:

```
RP/0/RP0/CPU0:router# show bgp all all count-only
```

```
Address Family: IPv4 Unicast
=====
```

```
BGP router identifier 10.0.0.1, local AS number 1
BGP generic scan interval 60 secs
BGP main routing table version 109
BGP scan interval 60 secs
```

```
Processed 8 prefixes, 8 paths
```

```
Address Family: IPv4 Multicast
=====
```

```
BGP router identifier 10.0.0.1, local AS number 1
BGP generic scan interval 60 secs
BGP main routing table version 15
BGP scan interval 60 secs
```

```
Processed 2 prefixes, 2 paths
```

```
Address Family: IPv6 Unicast
=====
```

```
BGP router identifier 10.0.0.1, local AS number 1
BGP generic scan interval 60 secs
BGP main routing table version 19
BGP scan interval 60 secs
```

```
Processed 2 prefixes, 2 paths
```

Table 10 describes the significant fields shown in the display.

Table 10 *show bgp count-only Field Descriptions*

Field	Description
BGP router identifier	BGP identifier for the local system.
local AS number	Autonomous system number for the local system.

R3.3 Beta Draft – Cisco Confidential Information

Table 10 ***show bgp count-only Field Descriptions (continued)***

Field	Description
BGP generic scan interval	Interval (in seconds) between scans for garbage collection across all address family-independent tables.
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
BGP scan interval	Interval (in seconds) between scans of the BGP table specified by the address family and subaddress family.
Processed n prefixes, n paths	Number of prefixes and number of paths processed for the table.

Related Commands

Command	Description
set default-afi	Sets the default Address Family Identifier (AFI) for the current session.
set default-safi	Sets the default Subaddress Family Identifier (SAFI) for the current session.

R3.3 Beta Draft—Cisco Confidential Information

show bgp dampened-paths

To display Border Gateway Protocol (BGP) dampened routes, use the **show bgp dampened-paths** command in EXEC mode.

```
show bgp [ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
[vpn4 unicast] [rd rd-address] | vrf {vrf-name | all} [ipv4 unicast]] dampened-paths
```

Syntax Description	
ipv4	(Optional) Specifies IP Version 4 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
all	(Optional) For subaddress families, specifies prefixes for all subaddress families.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
all	(Optional) For address family, specifies prefixes for all address families.
vpn4 unicast	(Optional) Specifies VPNv4 unicast address families.
rd rd-address	(Optional) Displays routes with a specific route distinguisher.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 unicast	(Optional) For VRF, specifies IPv4 unicast address families.

Defaults If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	The following keywords and arguments were added: vrf {vrf-name all} [ipv4 unicast] [vpn4 unicast] [rd rd-address]

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information



Note

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

BGP contains a separate routing table for each configured address family and subaddress family combination. The address family and subaddress family options specify the routing table to be examined. If the **all** keyword is specified for the address family or for the subaddress family, each matching routing table is examined in turn.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp dampened-paths** command in EXEC mode:

```
RP/0/RP0/CPU0:router# show bgp dampened-paths
```

```
BGP router identifier 10.2.0.1, local AS number 3
BGP generic scan interval 60 secs
BGP main routing table version 7
Dampening enabled
BGP scan interval 60 secs
Status codes:s suppressed, d damped, h history, * valid, > best
                i - internal, S stale
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network      From        Reuse      Path
*d 10.0.0.0      10.0.101.35    00:01:20  35 i
```

Table 11 describes the significant fields shown in the display.

Table 11 *show bgp dampened-paths Field Descriptions*

Field	Description
BGP router identifier	BGP identifier for the local system.
local AS number	Autonomous system number for the local system.
BGP generic scan interval	Interval (in seconds) between scans for garbage collection across all address family-independent tables.
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
Dampening enabled	Displayed if dampening is enabled for the routes in this BGP routing table.
BGP scan interval	Interval (in seconds) between scans of the BGP table specified by the address family and subaddress family.

R3.3 Beta Draft—Cisco Confidential Information

Table 11 *show bgp dampened-paths Field Descriptions (continued)*

Field	Description
Status codes	Status of the table entry. The status is displayed as a three-character field at the beginning of each line in the table. The first character may be (in order of precedence): S—Path is stale, indicating that a graceful restart is in progress with the peer from which the route was learned. s—Path is more specific than a locally sourced aggregate route and has been suppressed. *—Path is valid. The second character may be (in order of precedence): >—Path is the best path to use for that network. d—Path is dampened. h—Path is a history entry, representing a route that is currently withdrawn, but that is being maintained to preserve dampening information. Such routes should never be marked as valid. The third character may be: i—Path was learned by an internal BGP (iBGP) session.
Origin codes	Origin of the path. The origin code is displayed at the end of each line in the table. It can be one of the following values: i—Path originated from an Interior Gateway Protocol (IGP) and was advertised with a network or aggregate-address command. e—Path 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	IP prefix and prefix length for a network.
From	Neighbor from which the route was received.
Reuse	Time (in hours:minutes:seconds) after which the path is made available.
Path	Autonomous system path to the destination network. At the end of the path is the origin code for the path.

Related Commands

Command	Description
aggregate-address	Creates an aggregate entry in a BGP routing table.
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear bgp dampening	Clears BGP route dampening information and unsuppresses the suppressed routes.
network (BGP)	Specifies a local network that the BGP routing process should originate and advertise to its neighbors.
set default-afi	Sets the default Address Family Identifier (AFI) for the current session.

R3.3 Beta Draft – Cisco Confidential Information

set default-safi	Sets the default Subaddress Family Identifier (SAFI) for the current session.
show bgp flap-statistics	Displays BGP routes that have flapped.
show bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

R3.3 Beta Draft—Cisco Confidential Information

show bgp flap-statistics

To display information about Border Gateway Protocol (BGP) paths that have flapped, use the **show bgp flap-statistics** command in EXEC mode.

```
show bgp [ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
[vpn4 unicast] [rd rd-address] | vrf {vrf-name | all} [ipv4 unicast]] flap-statistics [regexp
regular-expression | route-policy route-policy-name | cidr-only | {ip-address [{mask |
/prefix-length} [longer-prefixes]] [detail]]]
```

Syntax Description

ipv4	(Optional) Specifies IP Version 4 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
all	(Optional) For subaddress families, specifies prefixes for all subaddress families.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
all	(Optional) For address family, specifies prefixes for all address families.
vpn4 unicast	(Optional) Specifies VPNv4 unicast address families.
rd rd-address	(Optional) Displays routes with a specific route distinguisher.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 unicast	(Optional) For VRF, specifies IPv4 unicast address families.
regexp <i>regular-expression</i>	(Optional) Displays flap statistics for all paths that match the regular expression.
route-policy <i>route-policy-name</i>	(Optional) Displays flap statistics for a route policy.
cidr-only	(Optional) Displays only routes whose prefix length does not match the classful prefix length for that network. The cidr-only keyword can be specified only if the address family is IPv4.
<i>ip-address</i>	(Optional) Flap statistics for a network address only.
<i>mask</i>	(Optional) Network mask applied to the <i>ip-address</i> argument.
<i>/prefix-length</i>	(Optional) Length of the IP address prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash (/) must precede the decimal value.
longer-prefixes	(Optional) Displays flap statistics for the specified prefix and more-specific prefixes. The longer-prefixes keyword is available when the <i>ip-address</i> and <i>mask</i> or <i>/prefix-length</i> arguments are specified.
detail	(Optional) Displays dampening parameters for the path. The detail keyword cannot be specified if the longer-prefixes keyword is specified. The detail keyword is available when the <i>ip-address</i> argument or <i>ip-address</i> and <i>mask</i> or <i>/prefix-length</i> arguments are specified.

R3.3 Beta Draft—Cisco Confidential Information

Defaults

If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The filter-list access-list keyword and argument were removed. The route-policy route-policy-name keyword and argument were added.
Release 3.3	The following keywords and arguments were added: • vrf {vrf-name all} [ipv4 unicast] • [vpngv4 unicast] [rd rd-address]

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.



Note

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

BGP contains a separate routing table for each configured address family and subaddress family combination. The address family and subaddress family options specify the routing table to be examined. If the **all** keyword is specified for the address family or subaddress family, each matching routing table is examined in turn.

Flap statistics are maintained only for paths if dampening is enabled using the **bgp dampening** command. If dampening is not enabled, the **show bgp flap-statistics** command does not display any paths.

If no arguments or keywords are specified, the software displays flap statistics for all paths for the specified address family. You can use the **regexp**, **filter-list**, **cidr-only**, and **longer-prefixes** options to limit the set of paths displayed.

If you specify a network address without a mask or prefix length, the longest matching prefix for the network address is displayed. When displaying flap statistics for a single route, use the **detail** keyword to display dampening parameters for the route.

Task ID

Task ID	Operations
bgp	read

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following is sample output from the **show bgp flap-statistics** command:

```
RP/0/RP0/CPU0:router# show bgp flap-statistics

BGP router identifier 172.20.1.1, local AS number 1820
BGP main routing table version 26180
Dampening enabled
BGP scan interval 60 secs
Status codes: s suppressed, d damped, h history, * valid, > best
                i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          From          Flaps Duration Reuse      Path
*d 10.0.0.0       172.20.16.177  4      00:13:31 00:18:10 100
*d 10.10.0.0      172.20.16.177  4      00:02:45 00:28:20 100
```

The following is sample output from the **show bgp flap-statistics** command with the **detail** keyword in EXEC mode:

```
RP/0/RP0/CPU0:router# show bgp flap-statistics 172.31.12.166 detail

BGP router identifier 10.0.0.5, local AS number 1
BGP main routing table version 738
Dampening enabled
BGP scan interval 60 secs
Status codes: s suppressed, d damped, h history, * valid, > best
                i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          From          Flaps Duration Reuse      Path
h 172.31.12.166  10.0.101.1    6      00:03:28                2 2000 3000

Half life        Suppress      Reuse penalty  Max. supp. time
00:15:00         2000         750           01:00:00
```

Table 12 describes the significant fields shown in the display.

Table 12 *show bgp flap-statistics Field Descriptions*

Field	Description
BGP route identifier	BGP identifier for the local system.
local AS number	Autonomous system number for the local system.
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
Dampening enabled	Displayed if dampening has been enabled for the routes in this BGP routing table.
BGP scan interval	Interval (in seconds) between scans of the BGP table specified by the address family and subaddress family.

R3.3 Beta Draft—Cisco Confidential Information

Table 12 *show bgp flap-statistics Field Descriptions (continued)*

Field	Description
Status codes	Status of the table entry. The status is displayed as a three-character field at the beginning of each line in the table. The first character may be (in order of precedence): S—Path is stale, indicating that a graceful restart is in progress with the peer from which the route was learned. s—Path is more specific than a locally sourced aggregate route and has been suppressed. *—Path is valid. The second character may be (in order of precedence): >—Path is the best path to use for that network. d—Path is dampened. h—Path is a history entry, representing a route that is currently withdrawn, but that is being maintained to preserve dampening information. Such routes should never be marked as valid. The third character may be: i—Path was learned by an internal BGP (iBGP) session.
Origin codes	Origin of the path. The origin code is displayed at the end of each line in the table. It can be one of the following values: i—Path originated from an Interior Gateway Protocol (IGP) and was advertised with a network or aggregate-address command. e—Path 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	IP prefix and prefix length for a network that is dampened.
From	IP address of the peer that advertised this route.
Flaps	Number of times the route has flapped.
Duration	Time (in hours:minutes:seconds) since the first flap.
Reuse	Time (in hours:minutes:seconds) after which the path is made available.
Path	Autonomous system path of the route that is being dampened.
Half life	Half-life value used when dampening this route. The half-life is the amount of time that must elapse to reduce the reuse penalty by half. The half-life value is specified using the bgp dampening command.
Suppress	Suppress value used to dampen this route. The suppress value is the value that the penalty must exceed for the route to be suppressed. The suppress value can be configured using the bgp dampening command.

R3.3 Beta Draft—Cisco Confidential Information

Table 12 *show bgp flap-statistics Field Descriptions (continued)*

Field	Description
Reuse penalty	Reuse penalty used to dampen this route. The penalty must fall below the reuse penalty for the route to be unsuppressed. The reuse penalty can be configured using the bgp dampening command.
Max supp. time	Maximum length of time that the route may be suppressed due to dampening. The maximum suppress time can be configured using the bgp dampening command.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
set default-afi	Sets the default Address Family Identifier (AFI) for the current session.
set default-safi	Sets the default Subaddress Family Identifier (SAFI) for the current session.
show bgp dampened-paths	Displays the BGP dampened routes.
show bgp neighbors	Displays information about BGP neighbors.

R3.3 Beta Draft—Cisco Confidential Information

show bgp inconsistent-as

To display Border Gateway Protocol (BGP) routes with inconsistent autonomous system paths, use the **show bgp inconsistent-as** command in EXEC mode.

```
show bgp [ipv4 { unicast | multicast | all } | ipv6 { unicast | all } | all { unicast | multicast | all } |
        [vpnv4 unicast] [rd rd-address] | vrf { vrf-name | all } [ipv4 unicast]] inconsistent-as
```

Syntax Description

ipv4	(Optional) Specifies IP Version 4 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
all	(Optional) For subaddress families, specifies prefixes for all subaddress families.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
all	(Optional) For address family, specifies prefixes for all address families.
vpnv4 unicast	(Optional) Specifies VPNv4 unicast address families.
rd rd-address	(Optional) Displays routes with a specific route distinguisher.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 unicast	(Optional) For VRF, specifies IPv4 unicast address families.

Defaults

If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	The following keywords and arguments were added: vrf { vrf-name all } [ipv4 unicast] [vpnv4 unicast] [rd rd-address]

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information



Note

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

BGP contains a separate routing table for each configured address family and subaddress family combination. The address family and subaddress family options specify the routing table to be examined. If the **all** keyword is specified for the address family or for the subaddress family, each matching routing table is examined in turn.

Use the **show bgp inconsistent-as** command to search through all prefixes in the specified BGP routing table and display the paths for any prefix that has inconsistent originating autonomous system numbers. The originating autonomous system is the last autonomous system number displayed in the path field and should be the same for all paths.

If a prefix has one or more paths originating from different autonomous systems, all paths for that prefix are displayed.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp inconsistent-as** command in EXEC mode:

```
RP/0/RP0/CPU0:router# show bgp inconsistent-as

BGP router identifier 172.20.1.1, local AS number 1820
BGP main routing table version 1129
BGP scan interval 60 secs
Status codes: s suppressed, d damped, h history, * valid, > best
                i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network        Next Hop        Metric        LocPrf Weight Path
* 10.0.0.0      172.16.232.55      0              0 300 88 90 99 ?
*>              172.16.232.52      2222           0 400 ?
* 172.16.0.0    172.16.232.55      0              0 300 90 99 88 200 ?
*>              172.16.232.52      2222           0 400 ?
* 192.168.199.0 172.16.232.55      0              0 300 88 90 99 ?
*>              172.16.232.52      2222           0 400 ?
```

Table 13 describes the significant fields shown in the display.

Table 13 *show bgp inconsistent-as Field Descriptions*

Field	Description
BGP router identifier	BGP identifier for the local system.
local AS number	Autonomous system number for the local system.
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
Dampening enabled	Displayed if dampening is enabled for the routes in this BGP routing table.

R3.3 Beta Draft—Cisco Confidential Information

Table 13 *show bgp inconsistent-as Field Descriptions (continued)*

Field	Description
BGP scan interval	Interval (in seconds) between scans of the BGP table specified by the address family and subaddress family.
Status codes	Status of the table entry. The status is displayed as a three-character field at the beginning of each line in the table. The first character may be (in order of precedence): S—Path is stale, indicating that a graceful restart is in progress with the peer from which the route was learned. s—Path is more specific than a locally sourced aggregate route and has been suppressed. *—Path is valid. The second character may be (in order of precedence): >—Path is the best path to use for that network. d—Path is dampened. h—Path is a history entry, representing a route that is currently withdrawn, but that is being maintained to preserve dampening information. Such routes should never be marked as valid. The third character may be: i—Path was learned by an internal BGP (iBGP) session.
Origin codes	Origin of the path. The origin code is displayed at the end of each line in the table. It can be one of the following values: i—Path originated from an Interior Gateway Protocol (IGP) and was advertised with a network or aggregate-address command. e—Path 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	IP prefix and prefix length for a network.
Next Hop	IP address of the next system that is used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network.
Metric	Value of the interautonomous system metric, otherwise known as the Multi Exit Discriminator (MED) metric.
LocPrf	Local preference value. This is used to determine the preferred exit point from the local autonomous system. It is propagated throughout the local autonomous system.
Weight	Path weight. Weight is used in choosing the preferred path to a route. It is not advertised to any neighbor.
Path	Autonomous system path to the destination network. At the end of the path is the origin code for the path.

R3.3 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	network (BGP)	Specifies a local network that the BGP routing process should originate and advertise to its neighbors.
	route-policy (BGP)	Applies a routing policy to updates advertised to or received from a BGP neighbor.
	set default-afi	Sets the default Address Family Identifier (AFI) for the current session.
	set default-safi	Sets the default Subaddress Family Identifier (SAFI) for the current session.

R3.3 Beta Draft—Cisco Confidential Information

show bgp neighbor-group

To display information about the Border Gateway Protocol (BGP) configuration for neighbor groups, use the **show bgp neighbor-group** command in EXEC mode.

show bgp neighbor-group *group-name* {**configuration** [**defaults**] [**nvgen**] | **inheritance** | **users**}

Syntax Description

<i>group-name</i>	Name of the address family group to display.
configuration	(Optional) Displays the effective configuration for the neighbor group, including any configuration inherited by this neighbor group.
defaults	(Optional) Displays all configuration, including default configuration.
nvgen	(Optional) Displays output in show running-config command output. Note If the defaults keyword is also specified, the output is not suitable for cutting and pasting into a configuration session.
inheritance	Displays the af-groups, session groups, and neighbor groups from which this neighbor group inherits configuration.
users	Displays the neighbors and neighbor groups that inherit configuration from this neighbor group.

Defaults

No default behavior or value

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show bgp neighbor-group** command with the *group-name* **configuration** argument and keyword to display the effective configuration of a neighbor group, including any configuration inherited from session groups, address family groups, and neighbor groups through application of the **use** command. The source of each configured command is also displayed.

Use the **defaults** keyword to display all configuration for the neighbor group, including default configuration. The command output identifies default configuration. Use the **nvgen** keyword to display configuration in the output form of **show running-config** command. Output in this form is suitable for cutting and pasting into a configuration session.

R3.3 Beta Draft—Cisco Confidential Information

The **show bgp neighbor-group** command with the *group-name inheritance* argument and keyword displays the session groups, address family groups, and neighbor groups from which the specified neighbor group inherits configuration.

The **show bgp neighbor-group** *group-name* command displays the neighbors and neighbor groups that inherit configuration from the specified neighbor group.

Task ID	Task ID	Operations
	bgp	read

Examples

The examples use the following configuration:

```
af-group group3 address-family ipv4 unicast
  remove-private-AS
  soft-reconfiguration inbound
!
af-group group2 address-family ipv4 unicast
  use af-group group3
  send-community-ebgp
  send-extended-community-ebgp
  capability orf prefix-list both
!
session-group group3
  dmzlink-bw
!
neighbor-group group3
  use session-group group3
  timers 30 90
!
neighbor-group group1
  remote-as 1982
  use neighbor-group group2
  address-family ipv4 unicast
!
!
neighbor-group group2
  use neighbor-group group3
  address-family ipv4 unicast
  use af-group group2
  weight 100
!
```

The following is sample output from the **show bgp neighbor-group** command with the **configuration** keyword:

```
RP/0/RP0/CPU0:router# show bgp neighbor-group group1 configuration
```

```
neighbor-group group1
  remote-as 1982                []
  timers 30 90                  [n:group2 n:group3]
  dmzlink-bw                     [n:group2 n:group3 s:group3]
  address-family ipv4 unicast    []
  capability orf prefix-list both [n:group2 a:group2]
  remove-private-AS              [n:group2 a:group2 a:group3]
  send-community-ebgp            [n:group2 a:group2]
  send-extended-community-ebgp   [n:group2 a:group2]
  soft-reconfiguration inbound   [n:group2 a:group2 a:group3]
  weight 100                     [n:group2]
```

R3.3 Beta Draft—Cisco Confidential Information

The configuration source is shown to the right of each command. In the output, the **remote-as** command is configured directly on neighbor group group1, and the **send-community-ebgp** command is inherited from neighbor group group2, which in turn inherits the setting from af-group group2.

The following is sample output from the **show bgp neighbor-group** command with the **users** keyword. This output shows that the group1 neighbor group inherits session (address family-independent configuration parameters) from the group2 neighbor group. The group1 neighbor group also inherits IPv4 unicast configuration parameters from the group2 neighbor group:

```
RP/0/RP0/CPU0:router# show bgp neighbor-group group2 users
```

```
Session:      n:group1
IPv4 Unicast: n:group1
```

The following is sample output from the **show bgp neighbor-group** command with the **inheritance** keyword. This output shows that the specified neighbor group group1 inherits session (address family-independent configuration) from neighbor group group2, which inherits its own session from neighbor group group3. Neighbor group group3 inherited its session from session group group3. It also shows that the group1 neighbor-group inherits IPv4 unicast configuration parameters from the group2 neighbor group, which in turn inherits them from the group2 af-group, which itself inherits them from the group3 af-group:

```
RP/0/RP0/CPU0:router# show bgp neighbor-group group1 inheritance
```

```
Session:      n:group2 n:group3 s:group3
IPv4 Unicast: n:group2 a:group2 a:group3
```

Table 14 describes the significant fields shown in the display.

Table 14 *show bgp neighbor-group Field Descriptions*

Field	Description
[]	Configures the command directly on the specified address family group.
s:	Indicates the name that follows is a session group.
a:	Indicates the name that follows is an address family group.
n:	Indicates the name that follows is a neighbor group.
[dflt]	Indicates the setting is not explicitly configured or inherited, and the default value for the setting is used. This field may be shown when the defaults keyword is specified.
<not set>	Indicates that the default is for the setting to be disabled. This field may be shown when the defaults keyword is specified.

Related Commands

Command	Description
af-group	Configures a BGP address family group.
session-group	Creates a session group and enters session group configuration mode.
show bgp af-group	Displays information about configuration for address family groups.
show bgp neighbors	Displays information about BGP neighbors, including configuration inherited from neighbor groups, session groups, and address family groups.
show bgp session-group	Displays information about the BGP configuration for session groups.

R3.3 Beta Draft—Cisco Confidential Information

Command	Description
show running-config	Displays the contents of the currently running configuration or a subset of that configuration.
use	Inherits configuration from a neighbor group, a session group, or an address family group.

R3.3 Beta Draft—Cisco Confidential Information

show bgp neighbors

To display information about Border Gateway Protocol (BGP) connections to neighbors, use the **show bgp neighbors** command in EXEC mode.

```
show bgp [ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
vpnv4 unicast | vrf {vrf-name | all} [ipv4 unicast]] neighbors [performance-statistics]
```

```
show bgp [ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
vpnv4 unicast | vrf {vrf-name | all} [ipv4 unicast]] neighbors ip-address [advertised-routes
| dampened-routes | flap-statistics | performance-statistics | received {prefix-filter | routes}
| routes]
```

```
show bgp neighbors ip-address [configuration [defaults] [nvgen] | inheritance]
```

Syntax Description	
ipv4	(Optional) Specifies IP Version 4 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
all	(Optional) For subaddress families, specifies prefixes for all subaddress families.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
all	(Optional) For address family, specifies prefixes for all address families.
vpnv4 unicast	(Optional) Specifies VPNv4 unicast address families.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 unicast	(Optional) For VRF, specifies IPv4 unicast address families.
performance-statistics	(Optional) Displays performance statistics relative to work done by the BGP process for this neighbor.
<i>ip-address</i>	(Optional) IP address of the BGP-speaking neighbor. If you omit this argument, all neighbors are displayed.
advertised-routes	(Optional) Displays all routes the router advertised to the neighbor.
dampened-routes	(Optional) Displays the dampened routes that are learned from the neighbor.
flap-statistics	(Optional) Displays flap statistics of the routes learned from the neighbor.
received {prefix-filter routes}	(Optional) Displays information received from the BGP neighbor. The options are: • prefix-filter—Displays the prefix list filter. • routes—Displays routes from the neighbor before inbound policy
routes	(Optional) Displays routes learned from the neighbor.
configuration	(Optional) Displays the effective configuration for the neighbor, including any settings that have been inherited from session groups, neighbor groups, or af-groups used by this neighbor.

R3.3 Beta Draft—Cisco Confidential Information

defaults	(Optional) Displays all configuration settings, including any default settings.
nvgen	(Optional) Displays output in the show running-config command output.
inheritance	(Optional) Displays the session groups, neighbor groups, and af-groups from which this neighbor inherits configuration settings.

Defaults

If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The received routes keyword was added.
Release 3.3	The following keywords and arguments were added: vrf {<i>vrf-name</i> all} [ipv4 unicast] vpn4 unicast

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.



Note

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

BGP contains a separate routing table for each configured address family and subaddress family combination. The address family and subaddress family options specify which routing table should be examined. If the **all** keyword is specified for address family or subaddress family, each matching routing table is examined in turn.

Use the **show bgp neighbors** command to display detailed information about all neighbors or a specific neighbor. Use the **performance-statistics** keyword to display information about the work related to specific neighbors done by the BGP process.

Use the **show bgp neighbors** command with the *ip-address* **received prefix-filter** argument and keyword to display the Outbound Route Filter (ORF) received from a neighbor.

Use the **advertised-routes** keyword to display a summary of the routes advertised to the specified neighbor.

R3.3 Beta Draft—Cisco Confidential Information

Use the **dampened-routes** keyword to display routes received from the specified neighbor that have been suppressed due to dampening. For more details, see the **show bgp dampened-paths** command.

To display information about flapping routes received from a neighbor, use the **flap-statistics** keyword. For more details, see the **show bgp flap-statistics** command.

To display the routes received from a neighbor, use the **routes** keyword. For more details, see the **show bgp** command.

Use the **show bgp neighbor** command with the *ip-address configuration* argument and keyword to display the effective configuration of a neighbor, including configuration inherited from session groups, neighbor groups, or af-groups through application of the **use** command. Use the **defaults** keyword to display the value of all configurations for the neighbor, including default configuration. Use the **nvgen** keyword to display configuration output format of the **show running-config** command. Output in this format is suitable for cutting and pasting into a configuration session. Use the **show bgp neighbors** command with the *ip-address inheritance* argument and keyword to display the session groups, neighbor groups, and af-groups from which the specified neighbor inherits configuration.

Task ID	Task ID	Operations
	bgp	read

Examples

The following is sample output from the **show bgp neighbors** command:

```
RP/0/RP0/CPU0:router# show bgp neighbors 10.0.101.1
```

```
BGP neighbor is 10.0.101.1, remote AS 2, local AS 1, external link
Description: routem neighbor
Remote router ID 10.0.101.1
BGP state = Established, up for 00:00:56
TCP open mode: passive only

BFD enabled (session initializing)
Last read 00:00:55, hold time is 180, keepalive interval is 60 seconds
DMZ-link bandwidth is 1000 Mb/s
Neighbor capabilities:
  Route refresh: advertised
  Address family IPv4 Unicast: advertised and received
  Address family IPv4 Multicast: advertised and received
Received 119 messages, 0 notifications, 0 in queue
Sent 119 messages, 22 notifications, 0 in queue
Minimum time between advertisement runs is 60 seconds
```

```
For Address Family: IPv4 Unicast
BGP neighbor version 137
Update group: 1.3
Community attribute sent to this neighbor
AF-dependant capabilities:
  Outbound Route Filter (ORF) type (128) Prefix-list:
    Send-mode: advertised
    Receive-mode: advertised
Route refresh request: received 0, sent 0
Policy for incoming advertisements is pass-all
Policy for outgoing advertisements is pass-all
5 accepted prefixes, 5 are bestpaths
Prefix advertised 3, suppressed 0, withdrawn 0, maximum limit 1000000
Threshold for warning message 75%
```

R3.3 Beta Draft—Cisco Confidential Information

```

For Address Family: IPv4 Multicast
  BGP neighbor version 23
  Update group: 1.2
  Route refresh request: received 0, sent 0
  Policy for incoming advertisements is pass-all
  Policy for outgoing advertisements is pass-all
  2 accepted prefixes, 2 are bestpaths
  Prefix advertised 0, suppressed 0, withdrawn 0, maximum limit 131072
  Threshold for warning message 75%

Connections established 9; dropped 8
Last reset 00:02:10, due to User clear requested (CEASE notification sent -
administrative reset)
Time since last notification sent to neighbor: 00:02:10
Error Code: administrative reset
Notification data sent:
  None

```

Table 15 describes the significant fields shown in the display.

Table 15 *show bgp neighbors Field Descriptions*

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number. If the neighbor is in the same autonomous system as the router, then the link between them is internal; otherwise, it is considered external.
Description	Neighbor specific description.
remote AS	Number of the autonomous system to which the neighbor belongs.
local AS	Autonomous system number of the local system.
internal link	Neighbor is an internal BGP peer.
external link	Neighbor is an external BGP peer.
Administratively shut down	Neighbor connection is disabled using the shutdown command.
remote router ID	Router ID (an IP address) of the neighbor.
Neighbor under common administration	Neighbor is internal or a confederation peer.
BGP state	Internal state of this BGP connection.
BFD enabled	Status of bidirectional forwarding detection.
TCP open mode	TCP mode used in establishing the BGP session.
Last read	Time since BGP last read a message from this neighbor.
hold time	Hold time (in seconds) used on the connection with this neighbor.
keepalive interval	Interval for sending keepalives to this neighbor.
DMZ-link bandwidth	DMZ link bandwidth for this neighbor.
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	Indicates that the local system supports the displayed address family capability. If “received” is displayed, the neighbor also supports the displayed address family.

R3.3 Beta Draft—Cisco Confidential Information

Table 15 *show bgp neighbors Field Descriptions (continued)*

Field	Description
Received	Number of messages received from this neighbor, the number of notification messages received and processed from this neighbor, and the number of messages that have been received, but not yet processed.
Sent	Number of messages sent to this neighbor, the number of notification messages generated to be sent to this neighbor, and the number of messages queued to be sent to this neighbor.
Minimum time between advertisement runs	Advertisement interval (in seconds) for this neighbor.
For Address Family	Information that follows is specific to the displayed address family.
BGP neighbor version	Last version of the BGP database that was sent to the neighbor for the specified address family.
Update group	Update group to which the neighbor belongs.
Route reflector client	Indicates that the local system is acting as a route reflector for this neighbor.
Inbound soft reconfiguration allowed	Indicates that soft reconfiguration is enabled for routes received from this neighbor. Note If the neighbor has route refresh capability, then soft configuration received-only routes are not stored by the local system unless “override route refresh” is displayed.
eBGP neighbor with no inbound or outbound policy: defaults to drop	Indicates that the neighbor does not have an inbound or outbound policy configured using the route-policy (BGP) command. Hence, no routes are accepted from or advertised to this neighbor.
Private AS number removed from updates to this neighbor	Indicates that remove-private-AS is configured on the specified address family for this neighbor.
NEXT_HOP is always this router	Indicates that next-hop-self is configured on the specified address family for this neighbor.
Community attribute sent to this neighbor	Indicates that send-community-ebgp is configured on the specified address family for this neighbor.
Extended community attribute sent to this neighbor	Indicates that send-extended-community-ebgp is configured on the specified address family for this neighbor.
Default information originate	Indicates that default-originate is configured on the specified address family for this neighbor, together with the policy used, if one was specified in the default-originate configuration. An indication of whether the default route has been advertised to the neighbor is also shown.
AF-dependant capabilities	BGP capabilities that are specific to a particular address family.

R3.3 Beta Draft—Cisco Confidential Information**Table 15** *show bgp neighbors Field Descriptions (continued)*

Field	Description
Outbound Route Filter	Neighbor has the Outbound Route Filter (ORF) capability for the specified address family. Details of the capabilities supported are also shown: Send-mode—"advertised" is shown if the local system can send an outbound route filter to the neighbor. "received" is shown if the neighbor can send an outbound route filter to the local system. Receive-mode—"advertised" is shown if the local system can receive an outbound route filter from the neighbor. "received" is shown if the neighbor can receive an outbound route filter from the local system.
Graceful Restart Capability	Indicates whether graceful restart capability has been advertised to and received from the neighbor for the specified address family.
Neighbor preserved the forwarding state during latest restart	Indicates that when the neighbor connection was last established, the neighbor indicated that it preserved its forwarding state for the specified address family.
Local restart time	Restart time (in seconds) advertised to this neighbor.
RIB purge time	RIB purge time (in seconds) used for graceful restarts.
Maximum stalepath time	Maximum time (in seconds) a path received from this neighbor may be marked as stale if the neighbor restarts.
Remote Restart time	Restart time received from this neighbor.
Route refresh request	Number of route refresh requests sent and received from this neighbor.
Outbound Route Filter (ORF)	"sent" indicates that an outbound route filter has been sent to this neighbor. "received" indicates that an outbound route filter has been received from this neighbor. Note A received outbound route filter may be displayed using the show bgp neighbors command with the received prefix-filter keywords.
First update is deferred until ORF or ROUTE-REFRESH is received	If the local system advertised the receive capability and the neighbor has advertised send capability, no updates are generated until specifically asked by the neighbor (using a ROUTE-REFRESH or ORF with immediate request).
Scheduled to send the Prefix-list filter	Indicates the local system is due to send an outbound route filter request in order to receive updates from the neighbor.
Inbound path policy	Indicates if an inbound path policy is configured.
Outbound path policy	Indicates if an outbound path policy is configured.
Incoming update prefix filter list	Indicates a prefix list is configured to filter inbound updates from the neighbor.
Default weight	Default weight for routes received from the neighbor.
Policy for incoming advertisements	Indicates a route policy is configured to be applied to inbound updates from the neighbor.
Policy for outgoing advertisements	Indicates a route policy is configured to be applied to outbound updates to the neighbor.
Status	Status of conditional advertisement map for this neighbor.

R3.3 Beta Draft—Cisco Confidential Information

Table 15 *show bgp neighbors Field Descriptions (continued)*

Field	Description
Type	Indicates whether the condition map selects routes that should be advertised, or routes that should not be advertised: Exist—Routes advertised if permitted by the condition route map. Non-exist—Routes advertised if denied by the condition route map.
accepted prefixes	Number of prefixes accepted.
Prefix advertised	Number of prefixes advertised to the neighbor during the lifetime of the current connection with the neighbor.
suppressed	Number of prefix updates that were suppressed because no transitive attributes changed from one best path to the next. Note Update suppression occurs only for external BGP neighbors.
withdrawn	Number of prefixes withdrawn from the neighbor during the lifetime of the current connection with the neighbor.
maximum limit	Maximum number of prefixes that may be received from the neighbor. If “(warning-only)” is displayed, a warning message is generated when the limit is exceeded, otherwise the neighbor connection is shut down when the limit is exceeded.
Threshold for warning message	Percentage of maximum prefix limit for the neighbor at which a warning message is generated.
Connections established	Number of times the router has established a BGP peering session with the neighbor.
dropped	Number of times that a good connection has failed or been taken down.
Last reset due to	Reason that the connection with the neighbor was last reset.
Time since last notification sent to neighbor	Amount of time since a notification message was last sent to the neighbor.
Error Code	Type of notification that was sent. The notification data, if any, is also displayed.
Time since last notification received from neighbor	Amount of time since a notification message was last received from the neighbor.
Error Code	Type of notification that was received. The notification data received, if any, is also displayed
External BGP neighbor may be up to <n> hops away	Indicates ebgp-multihop is configured for the neighbor.
External BGP neighbor not directly connected	Indicates that the neighbor is not directly attached to the local system.
Notification data sent:	Data providing more details on the error along with the error notification sent to the neighbor.

R3.3 Beta Draft—Cisco Confidential Information

The following is sample output from the **show bgp neighbors** command with the **advertised-routes** keyword:

```
RP/0/RP0/CPU0:router# show bgp neighbors 10.0.101.75 advertised-routes
```

```
Network      Next Hop    From
10.10.0.0/8  10.0.101.1  10.0.101.1
10.11.0.0/8  10.0.101.3  10.0.101.3
10.12.0.0/8  10.0.101.5  10.0.101.5
```

The following is sample output from the **show bgp neighbors** command with the **routes** keyword:

```
RP/0/RP0/CPU0:router# show bgp neighbors 172.20.16.178 routes
```

```
BGP router identifier 172.20.16.181, local AS number 1
BGP main routing table version 27
BGP scan interval 60 secs
Status codes: s suppressed, d damped, h history, * valid, > best
                i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric LocPrf Weight Path
*> 10.0.0.0   172.20.16.178    40             0 10 ?
*> 10.22.0.0  172.20.16.178    40             0 10 ?
```

Table 16 describes the significant fields shown in the display.

Table 16 *show bgp neighbors routes Field Descriptions*

Field	Description
BGP router identifier	BGP identifier for the local system.
local AS number	Autonomous system number for the local system.
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
Dampening enabled	Displayed if dampening is enabled for the routes in this BGP routing table.
BGP scan interval	Interval (in seconds) between scans of the BGP table specified by the address family and subaddress family.

R3.3 Beta Draft—Cisco Confidential Information

Table 16 *show bgp neighbors routes Field Descriptions (continued)*

Field	Description
Status codes	Status of the table entry. The status is displayed as a three-character field at the beginning of each line in the table. The first character may be (in order of precedence): S—Path is stale, indicating that a graceful restart is in progress with the peer from which the route was learned. s—Path is more specific than a locally sourced aggregate route and has been suppressed. *—Path is valid. The second character may be (in order of precedence): >—Path is the best path to use for that network. d—Path is dampened. h—Path is a history entry, representing a route that is currently withdrawn, but that is being maintained to preserve dampening information. Such routes should never be marked as valid. The third character may be: i—Path was learned by an internal BGP (iBGP) session.
Origin codes	Origin of the path. The origin code is displayed at the end of each line in the table. It can be one of the following values: i—Path originated from an Interior Gateway Protocol (IGP) and was advertised with a network or aggregate-address command. e—Path 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	IP prefix and prefix length for a network.
Next Hop	IP address of the next system that is used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network.
Metric	Value of the interautonomous system metric, otherwise known as the Multi Exit Discriminator (MED) metric.
LocPrf	Local preference value. This is used to determine the preferred exit point from the local autonomous system. It is propagated throughout the local autonomous system.
Weight	Path weight. Weight is used in choosing the preferred path to a route. It is not advertised to any neighbor.
Path	Autonomous system path to the destination network. At the end of the path is the origin code for the path.

R3.3 Beta Draft—Cisco Confidential Information

The following is sample output from the **show bgp neighbors** command with the **dampened-routes** keyword:

```
RP/0/RP0/CPU0:router# show bgp neighbors 10.0.101.1 dampened-routes
```

```
BGP router identifier 10.0.0.5, local AS number 1
BGP main routing table version 48
Dampening enabled
BGP scan interval 60 secs
Status codes: s suppressed, d damped, h history, * valid, > best
                i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          From          Reuse    Path
*d 10.0.0.0         10.0.101.1      00:59:30 2 100 1000 i
*d 11.0.0.0         10.0.101.1      00:59:30 2 100 1000 i
*d 12.0.0.0         10.0.101.1      00:59:30 2 100 1000 i
*d 13.0.0.0         10.0.101.1      00:59:30 2 100 1000 i
*d 14.0.0.0         10.0.101.1      00:59:30 2 100 1000 i
```

Table 17 describes the significant fields shown in the display.

Table 17 *show bgp neighbors dampened-routes Field Descriptions*

Field	Description
BGP router identifier	BGP identifier for the local system.
local AS number	Autonomous system number for the local system.
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
Dampening enabled	Displayed if dampening is enabled for the routes in this BGP routing table.
BGP scan interval	Interval (in seconds) between scans of the BGP table specified by the address family and subaddress family.
Status codes	Status of the table entry. The status is displayed as a three-character field at the beginning of each line in the table. The first character may be (in order of precedence): S—Path is stale, indicating that a graceful restart is in progress with the peer from which the route was learned. s—Path is more specific than a locally sourced aggregate route and has been suppressed. *—Path is valid. The second character may be (in order of precedence): >—Path is the best path to use for that network. d—Path is dampened. h—Path is a history entry, representing a route that is currently withdrawn, but that is being maintained to preserve dampening information. Such routes should never be marked as valid. The third character may be: i—Path was learned by an internal BGP (iBGP) session.

R3.3 Beta Draft—Cisco Confidential Information

Table 17 *show bgp neighbors dampened-routes Field Descriptions (continued)*

Field	Description
Origin codes	Origin of the path. The origin code is displayed at the end of each line in the table. It can be one of the following values: i—Path originated from an Interior Gateway Protocol (IGP) and was advertised with a network or aggregate-address command. e—Path 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	IP prefix and prefix length for a network.
From	Neighbor from which the route was received.
Reuse	Time (in hours:minutes:seconds) after which the path is made available.
Path	Autonomous system path to the destination network. At the end of the path is the origin code for the path.

The following is sample output from the **show bgp neighbors** command with the **flap-statistics** keyword:

```
RP/0/RP0/CPU0:router# show bgp neighbors 10.0.101.1 flap-statistics

BGP router identifier 10.0.0.5, local AS number 1
BGP main routing table version 48
Dampening enabled
BGP scan interval 60 secs
Status codes: s suppressed, d damped, h history, * valid, > best
                i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
  Network          From          Flaps Duration Reuse      Path
  h 10.1.0.0        10.0.101.1    5008  2d02h           2 5000 1000
  h 10.2.0.0        10.0.101.1    5008  2d02h           2 2000 3000
  h 10.2.0.0        10.0.101.1    5008  2d02h           2 9000 6000
  *d 10.0.0.0        10.0.101.1    5008  2d02h          00:59:30 2 100 1000
  h 10.0.0.0/16      10.0.101.1    5008  2d02h           2 100 102
  *d 10.11.0.0       10.0.101.1    5008  2d02h          00:59:30 2 100 1000
  *d 10.12.0.0       10.0.101.1    5008  2d02h          00:59:30 2 100 1000
  *d 10.13.0.0       10.0.101.1    5008  2d02h          00:59:30 2 100 1000
  *d 10.14.0.0       10.0.101.1    5008  2d02h          00:59:30 2 100 1000
  h 192.168.0.0/16   10.0.101.1    5008  2d02h           2 100 101
```

Table 18 describes the significant fields shown in the display.

Table 18 *show bgp neighbors flap-statistics Field Descriptions*

Field	Description
BGP route identifier	BGP identifier for the local system.
local AS number	Autonomous system number for the local system.
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
Dampening enabled	Displayed if dampening has been enabled for the routes in this BGP routing table.

R3.3 Beta Draft—Cisco Confidential Information

Table 18 *show bgp neighbors flap-statistics Field Descriptions*

Field	Description
BGP scan interval	Interval (in seconds) between when the BGP process scans for the specified address family and subaddress family.
Status codes	Status of the table entry. The status is displayed as a three-character field at the beginning of each line in the table. The first character may be (in order of precedence): S—Path is stale, indicating that a graceful restart is in progress with the peer from which the route was learned. s—Path is more specific than a locally sourced aggregate route and has been suppressed. *—Path is valid. The second character may be (in order of precedence): d—Path is dampened. h—Path is a history entry, representing a route that is currently withdrawn, but that is being maintained to preserve dampening information. Such routes should never be marked as valid. The third character may be: i—Path was learned by an internal BGP (iBGP) session.
Origin codes	Origin of the path. The origin code is displayed at the end of each line in the table. It can be one of the following values: i—Path originated from an Interior Gateway Protocol (IGP) and was advertised with a network command. e—Path 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	IP prefix and prefix length for a network.
From	IP address of the peer that advertised this route.
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 is made available.
Path	Autonomous system path to reach the destination network.

The following is sample output from the **show bgp neighbors** command with the **performance-statistics** keyword:

```
RP/0/RP0/CPU0:router# show bgp neighbors 10.0.101.2 performance-statistics

BGP neighbor is 10.0.101.2, remote AS 1
  Read 3023 messages (58639 bytes) in 3019 calls (time spent: 1.312 secs)
  Read throttled 0 times
  Processed 3023 inbound messages (time spent: 0.198 secs)
  Wrote 58410 bytes in 6062 calls (time spent: 3.041 secs)
```

R3.3 Beta Draft—Cisco Confidential Information

```
Processing write list: wrote 0 messages in 0 calls (time spent: 0.000 secs)
Processing write queue: wrote 3040 messages in 3040 calls (time spent: 0.055 secs)
```

```
Received 3023 messages, 0 notifications, 0 in queue
Sent 3040 messages, 0 notifications, 0 in queue
```

Table 19 describes the significant fields shown in the display.

Table 19 *show bgp neighbors performance-statistics Field Descriptions*

Field	Description
Read	Indicates the number of messages received from the neighbor, the total size of received messages, the number of read operations performed, and the real time spent (in seconds) by the process performing read operations for this neighbor.
Read throttled	Number of times that reading from the TCP connection to this neighbor has been throttled. Throttling is due to a backlog of messages that have been read but not processed.
inbound messages	Number of read messages that have been processed, and the real time spent processing inbound messages for this neighbor.
Wrote	Amount of data that has been sent to this neighbor, number of write operations performed, and the real time spent by the process performing write operations for this neighbor.
Processing write list	Number of messages written from the write list to this neighbor, number of times the write list has been processed, and real time spent processing the write list. Note Write lists typically contain only update messages.
Processing write queue	Number of messages written from the write queue to this neighbor, number of times the write queue has been processed, and real time spent processing the write queue.
Received	Number of messages received from this neighbor, number of notification messages received and processed from this neighbor, and number of messages that have been received, but not yet processed.
Sent	Number of messages sent to this neighbor, number of notification messages generated to be sent to this neighbor, and number of messages queued to be sent to this neighbor.

The following is sample output from the **show bgp neighbors** command with the **configuration** keyword:

```
RP/0/RP0/CPU0:router# show bgp neighbors 10.0.101.1 configuration

neighbor 10.0.101.1
  remote-as 2 []
  bfd fast-detect []
  address-family ipv4 unicast []
  policy pass-all in []
  policy pass-all out []
  address-family ipv4 multicast []
  policy pass-all in []
  policy pass-all out []
```

Table 20 describes the significant fields shown in the display.

R3.3 Beta Draft – Cisco Confidential Information**Table 20** *show bgp neighbors configuration Field Descriptions*

Field	Description
neighbor	IP address configuration of the neighbor.
remote-as	Remote autonomous system configured on the neighbor.
bfd fast-detect	BFD parameter configured on the neighbor.
address-family	Address family and subsequent address family configured on the router.
route-policy pass-all in	Route policy configured for inbound updates.
route-policy pass-all out	Route policy configured for outbound updates.

Related Commands-

Command	Description
clear bgp	Resets a BGP connection or session.
network (BGP)	Specifies a local network that the BGP routing process should originate and advertise to its neighbors.
route-policy (BGP)	Applies a routing policy to updates advertised to or received from a BGP neighbor.
set default-afi	Sets the default Address Family Identifier (AFI) for the current session.
set default-safi	Sets the default Subaddress Family Identifier (SAFI) for the current session.
show bgp	Displays entries in the BGP routing table.
show bgp dampened-paths	Displays BGP dampened routes.
show bgp flap-statistics	Displays BGP routes that have flapped.
show bgp neighbor-group	Displays information about the BGP configuration for neighbor groups.
show bgp neighbors	Displays information about BGP connections to neighbors, including received prefix filters.
shutdown (BGP)	Disables a neighbor without removing all of its configuration.

R3.3 Beta Draft—Cisco Confidential Information

show bgp paths

To display all the Border Gateway Protocol (BGP) paths in the database, use the **show bgp paths** command in EXEC mode.

show bgp paths [**detail**] [**debug**] [*regular-expression*] [

Syntax Description

detail	(Optional) Displays detailed attribute information.
debug	(Optional) Displays attribute process ID, hash bucket, and hash chain ID attribute information.
<i>regular-expression</i>	(Optional) Autonomous system path that matches the regular expression.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported On the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show bgp paths** command to display information about AS paths and the associated attributes with which the paths were received.

If no options are specified, all stored AS paths are displayed with the number of routes using each path.

**Note**

The AS path information is stored independently of the address family, making it possible that routes from different address families could be using the same path.

Use the *regular-expression* argument to limit the output to only those paths that match the specified regular expression.

Use the **detail** keyword to display detailed information on the attributes stored with the AS path.

Task ID

Task ID	Operations
bgp	read

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following is sample output from the **show bgp paths** command:

```
RP/0/RP0/CPU0:router# show bgp paths detail
```

Proc	Attributes	Refcount	Metric	Path
Spk 0	ORG AS LOCAL	7	0	i
Spk 0	ORG AS LOCAL COMM EXTCOMM	3	0	2 1 i
Spk 0	MET ORG AS	3	55	2 i
Spk 0	ORG AS	3	0	2 10 11 i
Spk 0	ORG AS COMM	3	0	2 10 11 i
Spk 0	MET ORG AS ATOM	3	2	2 3 4 ?
Spk 0	MET ORG AS	3	1	2 3 4 e
Spk 0	MET ORG AS	3	0	2 3 4 i

Table 21 describes the significant fields shown in the display.

Table 21 *show bgp paths Field Descriptions*

Field	Description
Proc	ID of the process in which the path is stored. This is always “Spk 0.”
Attributes	Attributes that are present. The following may appear: MET—Multi Exit Discriminator (MED) attribute is present. ORG—Origin attribute is present. AS—AS path attribute is present. LOCAL—Local preference attribute is present. AGG—Aggregator attribute is present. COMM—Communities attribute is present. ATOM—Atomic aggregate attribute is present. EXTCOMM—Extended communities attribute is present.
NeighborAS	Autonomous system number of the neighbor, or 0, if the path information originated locally.
Refcount	Number of routes using a path.
Metric	Value of the interautonomous system metric, otherwise known as the MED metric.
Path	Autonomous system path to the destination network. At the end of the path is the origin code for the path: i—Path originated from an Interior Gateway Protocol (IGP) and was advertised with a network or aggregate-address command. e—Path 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.

R3.3 Beta Draft—Cisco Confidential Information

show bgp policy

To display information about Border Gateway Protocol (BGP) advertisements under a proposed policy, use the **show bgp policy** command in EXEC mode.

```
show bgp [ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
[vpn4 unicast] [rd rd-address] | vrf {vrf-name | all} [ipv4 unicast]] policy [neighbor
ip-address] [sent-advertisements | [route-policy route-policy-name] [summary]
```

Syntax Description

ipv4	(Optional) Specifies IP Version 4 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
all	(Optional) For subaddress families, specifies prefixes for all subaddress families.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
all	(Optional) For address family, specifies prefixes for all address families.
vpn4 unicast	(Optional) Specifies VPNv4 unicast address families.
rd rd-address	(Optional) Displays routes with a specific route distinguisher.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 unicast	(Optional) For VRF, specifies IPv4 unicast address families.
neighbor	(Optional) Previews advertisements for a single neighbor.
<i>ip-address</i>	(Optional) IP address of a single neighbor.
sent-advertisements	(Optional) Displays the routes that have been advertised to neighbors. If a route has not yet been advertised to the neighbor, it is not shown.
route-policy	(Optional) Displays advertisements for an output route policy.
<i>route-policy-name</i>	(Optional) Name of the route policy.
summary	(Optional) Displays a summary of the BGP advertisements.

Defaults

Advertisements for all neighbors are displayed if the **neighbor ip-address** keyword and argument are not specified. If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Release	Modification
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The the unsuppress-map <i>map</i> keyword and argument were removed and the route-policy <i>route-policy-name</i> keyword and argument were added.
Release 3.3	The following keywords and arguments were added: • vrf {<i>vrf-name</i> all} [ipv4 unicast] • [vpn4 unicast] [rd <i>rd-address</i>]

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.



Note

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

BGP contains a separate routing table for each configured address family and subaddress family combination. The address family and subaddress family options specify the routing table to be examined. If the **all** keyword is specified for the address family or subaddress family, each matching routing table is examined in turn.

Use the **show bgp policy** command to display routes that would be advertised to neighbors under a proposed policy. Unlike in the **show bgp advertised** command, the information displayed reflects any modifications made to the routes when executing the specified policy.

Use the **neighbor** keyword to limit the output to routes advertised to a particular neighbor. Use the **sent-advertisements** keyword to change the output in two ways:

- If a policy is not specified explicitly, any policy configured on the neighbor (using the **route-policy (BGP)** command) is executed before displaying the routes.
- Only routes that have already been advertised to the neighbor (and not withdrawn) are displayed. Routes that have not yet been advertised are not displayed.

Use the **summary** keyword to display abbreviated output.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp policy** command with the **summary** keyword in EXEC mode:

```
RP/0/RP0/CPU0:router# show bgp policy summary
```

Network	Next Hop	From	Advertised to
172.16.1.0/24	10.0.101.1	10.0.101.1	10.0.101.2
			10.0.101.3

R3.3 Beta Draft—Cisco Confidential Information

```

172.17.0.0/16      0.0.0.0      Local      10.0.101.1
                  10.0.101.2
                  10.0.101.3

```

Table 22 describes the significant fields shown in the display.

Table 22 *show bgp policy summary Field Descriptions*

Field	Description
Network	IP prefix and prefix length for a network.
Next Hop	IP address of the next system that is used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network.
From	IP address of the peer that advertised this route.
Local	Indicates the route originated on the local system.
Local Aggregate	Indicates the route is an aggregate created on the local system.
Advertised to	Indicates the neighbors to which this route was advertised.

The following is sample output from the **show bgp policy** command in EXEC mode:

```

RP/0/RP0/CPU0:router# show bgp policy

11.0.0.0/24 is advertised to 10.4.101.1
  Path info:
    neighbor: Local      neighbor router id: 10.4.0.1
    valid local best
  Attributes after inbound policy was applied:
    next hop: 0.0.0.0
    MET ORG AS
    origin: IGP metric: 0
    aspath:
  Attributes after outbound policy was applied:
    next hop: 10.4.0.1
    MET ORG AS
    origin: IGP metric: 0
    aspath: 1

11.0.0.0/24 is advertised to 10.4.101.2
  Path info:
    neighbor: Local      neighbor router id: 10.4.0.1
    valid local best
  Attributes after inbound policy was applied:
    next hop: 0.0.0.0
    MET ORG AS
    origin: IGP metric: 0
    aspath:
  Attributes after outbound policy was applied:
    next hop: 10.4.0.1
    MET ORG AS
    origin: IGP metric: 0
    aspath:

11.0.0.0/24 is advertised to 10.4.101.3
  Path info:
    neighbor: Local      neighbor router id: 10.4.0.1
    valid local best
  Attributes after inbound policy was applied:
    next hop: 0.0.0.0

```

R3.3 Beta Draft—Cisco Confidential Information

```

MET ORG AS
origin: IGP metric: 0
aspath:
Attributes after outbound policy was applied:
next hop: 10.4.0.1
MET ORG AS
origin: IGP metric: 0
aspath:

12.0.0.0/24 is advertised to 10.4.101.2
Path info:
neighbor: 10.4.101.1      neighbor router id: 10.4.101.1
valid external best
Attributes after inbound policy was applied:
next hop: 10.4.101.1
ORG AS
origin: IGP neighbor as: 2
aspath: 2 3 4
Attributes after outbound policy was applied:
next hop: 10.4.101.1
ORG AS
origin: IGP neighbor as: 2
aspath:2 3 4

12.0.0.0/24 is advertised to 10.4.101.3
Path info:
neighbor: 10.4.101.1      neighbor router id: 10.4.101.1
valid external best
Attributes after inbound policy was applied:
next hop: 10.4.101.1
ORG AS
origin: IGP neighbor as: 2
aspath: 2 3 4
Attributes after outbound policy was applied:
next hop: 10.4.101.1
ORG AS
origin: IGP neighbor as: 2
aspath:2 3 4

```

Table 23 describes the significant fields shown in the display.

Table 23 *show bgp policy Field Descriptions*

Field	Description
Is advertised to	IP address of the peer to which this route is advertised. If the route is advertised to multiple peers, information is shown separately for each peer.
neighbor	IP address of the peer that advertised this route, or one of the following: Local—Route originated on the local system. Local Aggregate—Route is an aggregate created on the local system.
neighbor router id	BGP identifier for the peer, or the local system if the route originated on the local system.
Not advertised to any peer	Indicates the no-advertise well-known community is associated with this route. Routes with this community are not advertised to any BGP peers.

R3.3 Beta Draft—Cisco Confidential Information

Table 23 *show bgp policy Field Descriptions (continued)*

Field	Description
Not advertised to any EBGp peer	Indicates the no-export well-known community is associated with this route. Routes with this community are not advertised to external BGP peers, even if those peers are in the same confederation as the local router.
Not advertised outside the local AS	Indicates the local-AS well-known community is associated with this route. Routes with this community value are not advertised outside the local autonomous system or confederation boundary.
(Received from a RR-client)	Path was received from a route reflector client.
(received-only)	Path is not used for routing purposes. It is used to support soft reconfiguration, and records the path attributes before inbound policy was applied to a path received from a peer. A path marked “received-only” indicates that either the path was dropped by inbound policy, or that a copy of path information was created and then modified for routing use.
(received & used)	Indicates that the path is used both for soft reconfiguration and routing purposes. A path marked “(received & used)”, implies the path information was not modified by inbound policy.
valid	Path is valid.
redistributed	Path is locally sourced through redistribution.
aggregated	Path is locally sourced through aggregation.
local	Path is locally sourced through the network command.
confed	Path was received from a confederation peer.
best	Path is selected as best.
multipath	Path is one of multiple paths selected for load-sharing purposes.
dampinfo	Indicates dampening information: Penalty—Current penalty for this path. Flapped—Number of times the route has flapped. In—Time (hours:minutes:seconds) since the network first flapped. Reuse in—Time (hours:minutes:seconds) after which the path is available. This field is displayed only if the path is currently suppressed.

R3.3 Beta Draft—Cisco Confidential Information**Table 23** *show bgp policy Field Descriptions (continued)*

Field	Description
Attributes after inbound policy was applied	Displays attributes associated with the received route, after any inbound policy has been applied. AGG—Aggregator attribute is present. AS—AS path attribute is present. ATOM—Atomic aggregate attribute is present. COMM—Communities attribute is present. EXTCOMM—Extended communities attribute is present. LOCAL—Local preference attribute is present. MET—Multi Exit Discriminator (MED) attribute is present. next hop—IP address of the next system used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network. ORG—Origin attribute is present.
origin	Origin of the path: IGP—Path originated from an Interior Gateway Protocol (IGP) and was sourced by BGP using a network or aggregate-address command. EGP—Path originated from an Exterior Gateway Protocol. incomplete—Origin of the path is not clear; in example, a route that is redistributed into BGP from an IGP.
neighbor as	First autonomous system (AS) number in the AS path.
aggregator	Indicates that the path was received with the aggregator attribute. The AS number and router-id of the system that performed the aggregation are shown.
metric	Value of the interautonomous system metric, otherwise known as the MED metric.
localpref	Local preference value. This is used to determine the preferred exit point from the local autonomous system. It is propagated throughout the local autonomous system
aspath	AS path associated with the route.
community	Community attributes associated with the path. Community values are displayed in AA:NN format, except for the following well-known communities: Local-AS—Community with value 4294901812. Routes with this community value are not advertised outside the local autonomous system or confederation boundary. no-advertise—Community with value 4294901813. Routes with this community value are not advertised to any BGP peers. no-export—Community with value 4294901814. Routes with this community are not advertised to external BGP peers, even if those peers are in the same confederation as the local router.

R3.3 Beta Draft—Cisco Confidential Information

Table 23 *show bgp policy Field Descriptions (continued)*

Field	Description
Extended community	Extended community attributes associated with the path. For known extended community types, the following codes may be displayed: RT—Route target community SoO—Site of Origin community LB—Link Bandwidth community
Originator	Router ID of the originating router when route reflection is used.
Cluster lists	Router ID or cluster ID of all route reflectors through which the route has passed.
Attributes after outbound policy was applied	Displays attributes associated with the received route, after any outbound policy has been applied. AGG—Aggregator attribute is present. AS—AS path attribute is present. ATOM—Atomic aggregate attribute is present. COMM—Communities attribute is present. EXTCOMM—Extended communities attribute is present. LOCAL—Local preference attribute is present. MET—Multi Exit Discriminator (MED) attribute is present. next hop—IP address of the next system used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network. ORG—Origin attribute is present.

Related Commands

Command	Description
route-policy (BGP)	Applies an inbound or outbound routing policy to a neighbor.
set default-afi	Sets the default Address Family Identifier (AFI) for the current session.
set default-safi	Sets the default Subaddress Family Identifier (SAFI) for the current session.
show bgp advertised	Displays routes advertised to neighbors.
show bgp neighbors	Displays information about the TCP and BGP connections to neighbors.
show bgp route-policy	Displays BGP information about networks that match an outbound route policy.

R3.3 Beta Draft—Cisco Confidential Information

show bgp process

To display Border Gateway Protocol (BGP) process information, use the **show bgp process** command in EXEC mode.

```
show bgp [ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all}]  
process [performance-statistics] [detail]
```

Syntax Description	
ipv4	(Optional) Specifies IP Version 4.
unicast	(Optional) Specifies the unicast subaddress family.
multicast	(Optional) Specifies the multicast subaddress family.
all	(Optional) For subaddress families, specifies prefixes for all subaddress families.
ipv6	(Optional) Specifies IP Version 6.
all	(Optional) For address family, specifies prefixes for all address families.
performance-statistics	(Optional) Displays performance statistics relative to the work done by the specified process.
detail	(Optional) Specifies detailed process information.

Defaults	If no address family or subaddress family is specified, the default address family and subaddress family specified using the set default-afi and set default-safi commands are used.

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

**Note**

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

R3.3 Beta Draft—Cisco Confidential Information

Use the **show bgp process** command to display status and summary information for the Border Gateway Protocol (BGP) process. The output shows various global and address family-specific BGP configuration. A summary of the number of neighbors, update messages, and notification messages sent and received by the process is also displayed.

Use the **detail** keyword to display detailed process information. The detailed process information shows the memory used by each of various internal structure types.

Use the **performance-statistics** keyword to display a summary or detail of work done by the BGP processes. The summary display shows the real time spent performing certain operations and the time stamps for state transitions during initial convergence.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp process** command:

```
RP/0/RP0/CPU0:router# show bgp process
```

```
BGP Process Information
BGP is operating in STANDALONE mode
Autonomous System: 1
Router ID: 10.0.0.5 (manually configured)
Cluster ID: 10.0.0.5
Fast external fallover enabled
Neighbor logging is enabled
Enforce first AS enabled
Default local preference: 100
Default keepalive: 60
Update delay: 120
Generic scan interval: 60
```

```
Address family: IPv4 Unicast
Dampening is enabled
Client reflection is enabled
Scan interval: 60
Main Table Version: 150
IGP notification: IGP notified
```

```
Node          Process      Nbrs Estab Rst Upd-Rcvd Upd-Sent Nfn-Rcvd Nfn-Sent
node0_0_CPU0 Speaker      3      2  1      20      10       0        0
```

Table 24 describes the significant fields shown in the display.

Table 24 *show bgp process Field Descriptions*

Field	Description
BGP is operating in	Indicates BGP is operating in standalone mode. This is the only supported mode.
Autonomous System	Autonomous system number for the local system.
Router ID	BGP identifier assigned to the local system. If this is explicitly configured using the bgp router-id command, “manually configured” is displayed. If the router ID is not manually configured, it is determined from a global router ID. If no global ID is available, the router ID is shown as 0.0.0.0.

R3.3 Beta Draft – Cisco Confidential Information**Table 24** *show bgp process Field Descriptions (continued)*

Field	Description
Confederation ID	Confederation identifier for the local system.
Cluster ID	Cluster identifier for the local system. If this is manually configured using the bgp cluster-id command, “manually configured” is displayed.
Default metric	Default metric. This is controlled by the default-metric command.
Fast external fallover enabled	Indicates whether fast external fallover is enabled. This is controlled by the bgp fast-external-fallover disable command.
Neighbor logging enabled	Indicates whether logging of peer connection up and down transitions is enabled. This is controlled by the bgp log neighbor changes disable command.
Enforce first AS enabled	Indicates that strict checking of the first AS number in paths received from external BGP peers is enabled. This is controlled by the bgp enforce-first-as disable command.
iBGP to IGP redistribution	Indicates internal redistribution is enabled using the bgp redistribution-internal command.
Treating missing MED as worst	Indicates missing Multi Exit Discriminator (MED) metric values are treated as worst in the route selection algorithm. This is controlled by the bgp bestpath med missing-as-worst command.
Always compare MED is enabled	Indicates that the MED is always used during the route selection algorithm, even when paths are received from external BGP neighbors in different autonomous systems. This is controlled by the bgp bestpath med always command.
AS Path ignore is enabled	Indicates that the AS path length is ignored by the route selection algorithm. This is controlled by the bgp bestpath as-path ignore command.
Comparing MED from confederation peers	Indicates that the MED values are used in the route selection algorithm when comparing routes received from confederation peers. This is controlled by the bgp bestpath med confed command.
Comparing router ID for eBGP paths	Indicates that the router ID is used as a tiebreaker by the route selection algorithm when comparing identical routes received from different external BGP neighbors. This is controlled by the bgp bestpath compare-routerid command.
Default local preference	Default local preference value used for BGP routes. This is controlled by the bgp default local-preference command.
Default keepalive	Default keepalive interval. This is controlled by the timers bgp command.
Graceful restart enabled	Indicates that the graceful restart capability is enabled. The configuration commands affecting graceful restart behavior are: bgp graceful-restart , bgp graceful-restart purge-time , bgp graceful-restart stalepath-time , bgp graceful-restart restart-time , and bgp graceful-restart graceful-reset .
Update delay	Maximum time that a BGP process stays in read-only mode.
Generic scan interval	Interval (in seconds) between BGP scans for address family-independent tasks. This is controlled by the bgp scan-time command.
Dampening	Indicates whether dampening is enabled for the specified address family. This is controlled by the dampening command.

R3.3 Beta Draft—Cisco Confidential Information

Table 24 *show bgp process Field Descriptions (continued)*

Field	Description
Client reflection	Indicates whether client-to-client route reflection is enabled for the specified address family. This is controlled by the bgp client-to-client reflection disable command.
Scan interval	Interval (in seconds) between BGP scans for the given address family. This is controlled by the bgp scan-time command in address family configuration mode.
Main Table Version	Last version of the BGP database that was installed into the main routing table.
IGP notification	Indicates whether Interior Gateway Protocols (IGP) have been notified of BGP convergence for the specified address family.
Node	Node on which the process is executing.
Process	Type of BGP process.
Speaker	Speaker process. A speaker process is responsible for receiving, processing, and sending BGP messages to configured neighbors.
Nbrs	Number of neighbors for which the process is responsible.
Estab	Number of neighbors that have connections in the established state for this process.
Rst	Number of times this process was restarted.
Upd-Rcvd	Number of update messages received by the process.
Upd-Sent	Number of update messages sent by the process.
Nfn-Rcvd	Number of notification messages received by the process.
Nfn-Sent	Number of notification messages sent by the process.

The following is sample output from the **show bgp process** command with the **detail** keyword:

```
RP/0/RP0/CPU0:router# show bgp all all process detail
```

```
BGP Process Information
BGP is operating in STANDALONE mode
Autonomous System: 1
Router ID: 10.0.0.5 (manually configured)
Cluster ID: 10.0.0.5
Fast external fallover enabled
Neighbor logging is enabled
Enforce first AS enabled
Default local preference: 100
Default keepalive: 60
Update delay: 120
Generic scan interval: 60
```

```
BGP Speaker process: 0, location node0_0_0
Neighbors: 3, established: 2
```

	Sent	Received
Updates:	3	15
Notifications:	0	0
	Number	Memory Used
Attributes:	12	1104

R3.3 Beta Draft—Cisco Confidential Information

```

AS Paths:                10                400
Communities:             2                1080
Extended communities:    1                40
Route Reflector Entries:  0                0
Route-map Cache Entries:  0                0
Filter-list Cache Entries: 0                0
Next Hop Cache Entries:  2                80
Update messages queued:  0

Address family: IPv4 Unicast
Dampening is enabled
Client reflection is enabled
Main Table Version: 12
IGP notification: IGP notified

State: normal mode.
BGP Table Version: 12
Network Entries: 15, Soft Reconfig Entries: 0
Dampened Paths: 0, History Paths: 9

Prefixes:                Allocated        Freed
Paths:                   15                0
                        19                0

Prefixes:                Number           Memory Used
Paths:                   15                1230
                        19                760

```

Table 25 describes the significant fields shown in the display.

Table 25 *show bgp process detail Field Descriptions*

Field	Description
BGP is operating in	Indicates whether BGP is operating in standalone mode.
Autonomous System	Autonomous system number for the local system.
Router ID	BGP identifier assigned to the local system. If this is explicitly configured using the bgp router-id command, “manually configured” is displayed. If the router ID is not manually configured, it is determined from a global router ID. If the global ID is not available, the router ID is shown as 0.0.0.0.
Confederation ID	Confederation identifier for the local system.
Cluster ID	Cluster identifier for the local system. If this is manually configured using the bgp cluster-id command, “manually configured” is displayed.
Default metric	Default metric.
Fast external fallover enabled	Indicates whether fast external fallover is enabled.
Neighbor logging enabled	Indicates whether logging of peer connection up and down transitions is enabled.
Enforce first AS enabled	Indicates that strict checking of the first autonomous system (AS) number in paths received from external BGP peers is enabled.
iBGP to IGP redistribution	Indicates internal redistribution is enabled using the bgp redistribution-internal command.

R3.3 Beta Draft—Cisco Confidential Information

Table 25 *show bgp process detail Field Descriptions (continued)*

Field	Description
Treating missing MED as worst	Indicates missing MED metric values are treated as worst in the route selection algorithm. This is controlled by the bgp bestpath med missing-as-worst command.
Always compare MED is enabled	Indicates that the MED is always used during the route selection algorithm, even when paths are received from external BGP neighbors in different autonomous systems. This is controlled by the bgp bestpath med always command.
AS Path ignore is enabled	Indicates that the AS path length is ignored by the route selection algorithm. This is controlled by the bgp bestpath as-path ignore command.
Comparing MED from confederation peers	Indicates that the MED values are used in the route selection algorithm when comparing routes received from confederation peers. This is controlled by the bgp bestpath med confed command.
Comparing router ID for eBGP paths	Indicates that the router ID is used as a tiebreaker by the route selection algorithm when comparing identical routes received from different external BGP neighbors. This is controlled by the bgp bestpath compare-routerid command.
Default local preference	Default local preference value used for BGP routes.
Default keepalive	Default keepalive interval. This is controlled by the timers bgp command.
Graceful restart enabled	Indicates that the graceful restart capability is enabled. The configuration commands affecting graceful restart behavior are: bgp graceful-restart , bgp graceful-restart purge-time , bgp graceful-restart stalepath-time , bgp graceful-restart restart-time , and bgp graceful-restart graceful-reset .
Update delay	Maximum time that a BGP process stays in read-only mode.
Generic scan interval	Interval (in seconds) between BGP scans for address family-independent tasks. This is controlled by the bgp scan-time command.
BGP Speaker Process	Speaker process responsible for receiving, processing and sending BGP messages.
Node	Node on which the specified process is executing.
Neighbors	Number of neighbors for which the specified process is responsible.
established	Number of neighbors that have connections in the established state for the specified process.
Updates	Number of update messages sent and received by the specified process.
Notifications	Number of notification messages sent and received by the specified process.
Attributes	Number of unique sets of attribute information stored in the specified process and the amount of memory used by the attribute information.
AS Paths	Number of unique autonomous system paths stored in the specified process and the amount of memory used by the AS path information.
Communities	Number of unique sets of community information stored in the specified process and the amount of memory used by them.
Extended communities	Number of unique sets of extended community information stored in the specified process and the amount of memory used by them.

R3.3 Beta Draft—Cisco Confidential Information**Table 25** *show bgp process detail Field Descriptions (continued)*

Field	Description
Route Reflector Entries	Number of unique sets of route reflector information stored in the specified process and the amount of memory used by them.
Nexthop Entries	Number of entries and memory usage for cached next hop information.
Update messages queued	Total number of update messages queued to be sent across all neighbors for which the specified process is responsible.
Address family	Specified address family.
Dampening	Indicates whether dampening is enabled for the specified address family.
Client reflection	Indicates whether client-to-client route reflection is enabled for the specified address family. This is controlled by the bgp client-to-client reflection disable command.
Scan interval	Interval (in seconds) between BGP scans for the given address family. This is controlled by the bgp scan-time command.
Main Table Version	Last version of the local BGP database for the specified address family that was injected into the main routing table.
IGP notification	Indicates whether IGP has been notified of BGP convergence for the specified address family.
RIB has converged	Indicates whether the main routing table version has converged and the version at which it converged.
State	BGP system state for the specified address family and process. This may be one of the following: read only mode—Initial set of updates is being recovered. In this mode, route selection is not performed, routes are not installed in the global RIB, and updates are not advertised to peers. best path calculation mode—Route selection is being performed for the routes that were received while in read-only mode. RIB update mode—Routes that were selected in best path calculation mode are being installed in the global RIB. normal mode—Route selection and RIB update are performed as updates are received.
BGP Table Version	Last version used in the BGP database for received routes.
Attribute download	Indicates whether the RIB attribute download is enabled.
Network Entries	Number of sets of prefix information held in the specified BGP process for the specified address family.
Soft Reconfig Entries	Number of sets of prefix information that are present only for the purpose of supporting soft reconfiguration.
Dampened Paths	Number of routes that are suppressed due to dampening for the specified address family.
History Paths	Number of routes that are currently withdrawn, but are being maintained to preserve dampening information.
Prefixes (Allocated/Freed)	Number of sets of prefix information for the specified address family that have been allocated and freed during the lifetime of the process.

R3.3 Beta Draft—Cisco Confidential Information

Table 25 *show bgp process detail Field Descriptions (continued)*

Field	Description
Paths (Allocated/Freed)	Number of sets of route information for the specified address family that have been allocated and freed during the lifetime of the process.
Prefixes (Number/Memory Used)	Number of sets of prefix information currently allocated for the specified address family, and the amount of memory used by them.
Paths (Number/Memory Used)	Number of sets of route information currently allocated for the specified address family, and the amount of memory used by them.

The following is sample output from the **show bgp process** command with the **performance-statistics** keyword:

```
RP/0/RP0/CPU0:router# show bgp process performance-statistics
```

```
BGP Process Information
BGP is operating in STANDALONE mode
Autonomous System: 1
Router ID: 10.0.0.5 (manually configured)
Cluster ID: 10.0.0.5
Fast external fallover enabled
Neighbor logging is enabled
Enforce first AS enabled
Default local preference: 100
Default keepalive: 60
Update delay: 120
Generic scan interval: 60
```

```
Address family: IPv4 Unicast
Dampening is not enabled
Client reflection is enabled
Scan interval: 60
Main Table Version: 10
IGP notification: IGP notified
RIB has converged: version 0
```

```
Address family: IPv4 Multicast
Dampening is not enabled
Client reflection is enabled
Scan interval: 60
Main Table Version: 3
RIB has converged: version 0
```

```
Address family: IPv6 Unicast
Dampening is not enabled
Client reflection is enabled
Scan interval: 60
Main Table Version: 3
RIB has converged: version 0
```

```
Address family: IPv6 Multicast
Dampening is not enabled
Client reflection is enabled
Scan interval: 60
Main Table Version: 1
RIB has converged: version 0
```

R3.3 Beta Draft—Cisco Confidential Information

```
Node          Process      Read      Write      Inbound
node0_0_CPU0  Speaker      0.09      0.03      0.04
```

Address Family IPv4 Unicast:

```
Process      Conv  Nbr Estab  Bestpath  RIB Inst  Read/Write  Last Upd
Speaker      No    0         120       120       120       121
```

Address Family IPv4 Multicast:

```
Process      Conv  Nbr Estab  Bestpath  RIB Inst  Read/Write  Last Upd
Speaker      Yes   0         120       120       120       121
```

Address Family IPv4 Multicast converged in 121 seconds.

Address Family IPv6 Unicast:

```
Process      Conv  Nbr Estab  Bestpath  RIB Inst  Read/Write  Last Upd
Speaker      Yes   0         120       120       120       121
```

Address Family IPv6 Unicast converged in 121 seconds.

Address Family IPv6 Multicast:

```
Process      Conv  Nbr Estab  Bestpath  RIB Inst  Read/Write  Last Upd
Speaker      No    0         120       120       120       ---
```

Table 26 describes the significant fields shown in the display.

Table 26 *show bgp process performance-statistics Field Descriptions*

Field	Description
BGP is operating in	Indicates whether BGP is operating in standalone mode.
Autonomous system	Autonomous system number for the local system.
Router ID	BGP identifier assigned to the local system. If this is explicitly configured using the bgp router-id command, “manually configured” is displayed. If the router ID is not manually configured, it is determined from a global router ID. If the global ID is not available, the router ID is shown as 0.0.0.0.
Confederation ID	Confederation identifier for the local system.
Cluster ID	The cluster identifier for the local system. If this is manually configured using the bgp cluster-id command, “manually configured” is displayed.
Default metric	Default metric.
Fast external fallover enabled	Indicates whether fast external fallover is enabled.
Neighbor logging enabled	Indicates whether logging of peer connection up and down transitions is enabled. This is controlled by the bgp log neighbor changes disable command.
Enforce first AS enabled	Indicates that strict checking of the first AS number in paths received from external BGP peers is enabled.

R3.3 Beta Draft—Cisco Confidential Information

Table 26 *show bgp process performance-statistics Field Descriptions (continued)*

Field	Description
iBGP to IGP redistribution	Indicates internal redistribution is enabled using the bgp redistribution-internal command.
Treating missing MED as worst	Indicates missing MED metric values are treated as worst in the route selection algorithm. This is controlled using the bgp bestpath med missing-as-worst command.
Always compare MED is enabled	Indicates that the MED is always used during the route selection algorithm, even when paths are received from external BGP neighbors in different autonomous systems. This setting is controlled by the bgp bestpath med always command.
AS Path ignore is enabled	Indicates that the AS path length is ignored by the route selection algorithm. This is controlled by the bgp bestpath as-path ignore command.
Comparing MED from confederation peers	Indicates that the MED values are used in the route selection algorithm when comparing routes received from confederation peers. This is controlled by the bgp bestpath med confed command.
Comparing router ID for eBGP paths	Indicates that the router ID is used as a tiebreaker by the route selection algorithm when comparing identical routes received from different external BGP neighbors. This is controlled by the bgp bestpath compare-routerid command.
Default local preference	Default local preference value used for BGP routes.
Default keepalive	Default keepalive interval. This setting is controlled by the timers bgp command.
Graceful restart enabled	Indicates that the graceful restart capability is enabled. The configuration commands affecting graceful restart behavior are: bgp graceful-restart , bgp graceful-restart purge-time , bgp graceful-restart stalepath-time , bgp graceful-restart restart-time , and bgp graceful-restart graceful-reset .
Update delay	Maximum time that a BGP process stays in read-only mode.
Generic scan interval	Interval (in seconds) between BGP scans for address family-independent tasks. This setting is controlled by the bgp scan-time command in router configuration mode.
Address family	Specified address family.
Dampening	Indicates whether dampening is enabled for the specified address family.
Client reflection	Indicates whether client-to-client route reflection is enabled for the specified address family. This is controlled by the bgp client-to-client reflection disable command.
Scan interval	Interval (in seconds) between BGP scans for the given address family. This is controlled by the bgp scan-time command.
Main Table Version	Last version of the local BGP database for the specified address family that was injected into the main routing table.
IGP notification	Indicates whether IGP has been notified of BGP convergence for the specified address family.
Node	Node on which the process is executing.
Process	BGP process.

R3.3 Beta Draft—Cisco Confidential Information

Table 26 *show bgp process performance-statistics Field Descriptions (continued)*

Field	Description
Speaker	Speaker process. The speaker process is responsible for receiving, processing and sending BGP messages.
Read	Real time (in seconds) spent reading messages from peers by this process.
Write	Real time (in seconds) spent writing messages to peers by this process.
Inbound	The real time (in seconds) spent processing messages read from peers by this process.
Config	Real time (in seconds) spent processing configuration commands by this process.
Data	Real time (in seconds) spent providing operational data by this process.
Conv	Indicates whether the process has converged after the initial update.
Nbr Estab	Time stamp (in seconds) recording the time when the first neighbor became established.
Bestpath	Time stamp (in seconds) recording the time the best path calculation mode was entered.
RIB Inst	Time stamp (in seconds) recording the time RIB update mode was entered.
Read/Write	Time stamp (in seconds) recording the time normal mode was entered.
Last Upd	Time stamp (in seconds) recording the time the last update was sent to a neighbor.
Address Family IPv4 Unicast converged in <i>n</i> seconds	Indicates that BGP has reached initial convergence for the IPv4 unicast address family. The time taken for convergence is shown.
Address Family IPv6 Multicast converged in <i>n</i> seconds	Indicates that BGP has reached initial convergence for the IPv6 multicast address family. The time taken for convergence is shown.

The following is sample output from the **show bgp process** command with the **performance-statistics** and **detail** keywords:

```
RP/0/RP0/CPU0:router# show bgp process performance-statistics detail
```

```
BGP Speaker process: 0, Node: node0_0_CPU0
Restart count: 2
Neighbors: 3, established: 2
```

	Sent	Received
Updates:	20	20
Notifications:	0	0

	Number	Memory Used
Attributes:	2	184
AS Paths:	2	48
Communities:	0	0
Extended communities:	0	0
Route Reflector Entries:	0	0
Route-map Cache Entries:	0	0
Filter-list Cache Entries:	0	0
Next Hop Cache Entries:	2	80
Update messages queued:	0	

R3.3 Beta Draft—Cisco Confidential Information

```

Read 14 messages (1142 bytes) in 12 calls (time spent: 0.024 secs)
Read throttled 0 times
Processed 14 inbound messages (time spent: 0.132 secs)
Wrote 2186 bytes in 24 calls (time spent: 0.024 secs)
Processing write list: wrote 18 messages in 4 calls (time spent: 0.000 secs)
Processing write queue: wrote 10 messages in 20 calls (time spent: 0.000 secs)
Socket setup (LPTS): 4 calls (time spent: 0.010 secs)
Configuration: 1 requests (time spent: 0.002 secs)
Operational data: 9 requests (time spent: 0.026 secs)

State: normal mode.
BGP Table Version: 150
Network Entries: 149, Soft Reconfig Entries: 0

Prefixes:           Allocated      Freed
Paths:              149             0

Prefixes:           Number          Memory Used
Paths:              200             8000

Updates generated: 149 prefixes in 8 messages from 2 calls (time spent: 0.046 secs)
Scanner: 2 scanner runs (time spent: 0.008 secs)
RIB update: 1 rib update runs, 149 prefixes installed (time spent: 0.024 secs)
Process has converged for IPv4 Unicast.

First neighbor established: 1082604050s
Entered DO_BESTPATH mode: 1082604055s
Entered DO_RIBUPD mode: 1082604055s
Entered Normal mode: 1082604055s
Latest UPDATE sent: 1082604056s

```

Table 27 describes the significant fields shown in the display.

Table 27 *show bgp process performance-statistics detail Field Descriptions*

Field	Description
Process	The specified process.
Location	Node in which the specified process is executing.
Neighbors	Number of neighbors for which the specified process is responsible.
established	Number of neighbors that have connections in the established state for the specified process.
Updates	Number of update messages sent and received by the specified process.
Notifications	Number of notification messages sent and received by the specified process.
Attributes	Number of unique sets of attribute information stored in the specified process and the amount of memory used by the attribute information.
AS Paths	Number of unique autonomous system paths stored in the specified process, and the amount of memory used by the AS path information.
Communities	Number of unique sets of community information stored in the specified process and the amount of memory used by them.

R3.3 Beta Draft – Cisco Confidential Information**Table 27** *show bgp process performance-statistics detail Field Descriptions (continued)*

Field	Description
Extended communities	Number of unique sets of extended community information stored in the specified process and the amount of memory used by them.
Route Reflector Entries	Number of unique sets of route reflector information stored in the specified process and the amount of memory used by them.
Route-map Cache Entries	Number of entries and memory usage for cached results for applying a route map.
Filter-list Cache Entries	Number of entries and memory usage for cached results for applying an AS path filter list.
Next Hop Cache Entries	Number of entries and memory usage for cached next hop information.
Update messages queued	Number of update messages queued to be sent across all neighbors for which the specified process is responsible.
Read	Indicates the number of messages read by the process, the total size of read messages, the number of read operations performed, and the real time spent by the process performing read operations.
Read throttled	Number of times that reading from TCP has been throttled due to a backlog of messages read but not processed.
inbound messages	Number of read messages that have been processed and the real time spent processing inbound messages.
Wrote	Amount of data that has been written by the process, the number of write operations performed, and the real time spent by the process performing write operations.
Processing write list	Number of messages written from write lists, the number of times the write list has been processed, and the real time spent processing the write list. Note Write lists typically contain only update messages.
Processing write queue	Number of messages written from write queues, number of times the write queue has been processed, and the real time spent processing the write queue.
Socket setup	Number of socket setup operations performed and the real time spent during socket setup operations.
Configuration	Number of configuration requests received by the process and the real time spent processing configuration requests.
Operational data	Number of requests for operational data (for show commands) received by the process and the real time spent processing operation data requests

R3.3 Beta Draft—Cisco Confidential Information

Table 27 *show bgp process performance-statistics detail Field Descriptions (continued)*

Field	Description
State	BGP system state for the specified address family and process. State may be one of the following: read only mode—Initial set of updates being received. In this mode, route selection is not performed, routes are not installed in the global RIB, and updates are not advertised to peers. best path calculation mode—Route selection is being performed for the routes that were received while in read-only mode. RIB update mode—Routes that were selected in best path calculation mode are being installed in the global RIB. normal mode—Route selection and RIB update are performed as updates are received.
BGP Table Version	Last version used in the BGP database for received routes.
Network Entries	Number of sets of prefix information held in the specified BGP process for the specified address family.
Soft Reconfig Entries	Number of sets of prefix information that are present only for the purpose of supporting soft reconfiguration.
Dampened Paths	Number of routes that are suppressed due to dampening for the specified address family.
History Paths	Number of routes that are currently withdrawn, but are being maintained to preserve dampening information.
Prefixes (Allocated/Freed)	Number of sets of prefix information for the specified address family that have been allocated and freed during the lifetime of the process.
Paths (Allocated/Freed)	Number of sets of route information for the specified address family that have been allocated and freed during the lifetime of the process.
Prefixes (Number/Memory Used)	Number of sets of prefix information currently allocated for the specified address family and amount of memory used by them.
Paths (Number/Memory Used)	Number of sets of route information currently allocated for the specified address family and amount of memory used by them.
Updates generated	Number of prefixes for which updates have been generated, the number of messages used to advertise the updates, the number of update generation runs performed, and the real time spent generating updates for the specified address family.
Scanner	Number of times the scanner has run for the specified address family and real time spent in scanner processing.
RIB Update	Number of global routing information base update runs performed for the specified address family, number of prefixes installed, withdrawn, or modified in the global RIB during these runs, and real time spent performing these runs.
Process has converged	Indicates whether the process has reached initial convergence for the specified address family.

R3.3 Beta Draft – Cisco Confidential Information**Table 27** *show bgp process performance-statistics detail Field Descriptions (continued)*

Field	Description
First neighbor established	Time stamp (in seconds) recording the time the first neighbor in the process was established.
Entered DO_BESTPATH mode	Time stamp (in seconds) recording the time best path calculation mode was entered.
Entered DO_RIBUPD mode	Time stamp (in seconds) recording the time RIB update mode was entered.
Entered Normal mode	Time stamp (in seconds) recording the time normal mode was entered.
Last UPDATE sent	Time stamp (in seconds) recording the time the last update was sent to a neighbor.

Related Commands

Command	Description
bgp bestpath as-path ignore	Sets the autonomous system path length to ignore when calculating preferred paths.
bgp bestpath compare-routerid	Compare identical routes received from external BGP (eBGP) peers during the best path selection process and select the route with the lowest router ID.
bgp bestpath med always	Compare the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems.
bgp bestpath med missing-as-worst	Assume paths with no MED attribute have the most undesirable MED value possible when performing path selection.
bgp cluster-id	Enables reflection of routes between route reflector clients using a BGP route reflector.
bgp cluster-id	Configure the cluster ID if the BGP cluster has more than one route reflector.
bgp default local-preference	Sets the default local preference value.
bgp redistribute-internal	Allows the redistribution of iBGP routes into an IGP such as Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF).
bgp router-id	Configures a fixed router ID for a BGP-speaking router.
default-metric (BGP)	Sets default metric values for the BGP.
set default-afi	Sets the default Address Family Identifier (AFI) for the current session.
set default-safi	Sets the default Subaddress Family Identifier (SAFI) for the current session.
bgp scan-time	Configures scanning intervals.
timers bgp	Sets default BGP timers.

R3.3 Beta Draft—Cisco Confidential Information

show bgp regexp

To display routes matching the autonomous system path regular expression, use the **show bgp regexp** command in EXEC mode.

```
show bgp [ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
vpnv4 unicast | vrf {vrf-name | all} [ipv4 unicast]] regexp regular-expression
```

Syntax Description		
ipv4	(Optional)	Specifies IP Version 4 address prefixes.
unicast	(Optional)	Specifies unicast address prefixes.
multicast	(Optional)	Specifies multicast address prefixes.
all	(Optional)	For subaddress families, specifies prefixes for all subaddress families.
ipv6	(Optional)	Specifies IP Version 6 address prefixes.
all	(Optional)	For address family, specifies prefixes for all address families.
vpnv4 unicast	(Optional)	Specifies VPNv4 unicast address families.
vrf	(Optional)	Specifies VPN routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional)	Name of a VRF.
all	(Optional)	For VRF, specifies all VRFs.
ipv4 unicast	(Optional)	For VRF, specifies IPv4 unicast address families.
<i>regular-expression</i>		Regular expression to match the BGP autonomous system paths.

Defaults If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	The following keywords and arguments were added: vrf {vrf-name all} [ipv4 unicast] vpnv4 unicast

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information



Note

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

BGP contains a separate routing table for each configured address family and subaddress family combination. The address family and subaddress family options specify the routing table to be examined. If the **all** keyword is specified for the address family or subaddress family, each matching routing table is examined in turn.

Use the **show bgp regexp** command to display all routes in the specified BGP table whose autonomous system path is matched by the specified regular expression.



Note

If the regular expression contains spaces, it must be specified and surrounded by quotation marks.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp regexp** command:

```
RP/0/RP0/CPU0:router# show bgp regexp "^3 "
```

BGP router identifier 10.0.0.5, local AS number 1
 BGP main routing table version 64
 BGP scan interval 60 secs
 Status codes: s suppressed, d damped, h history, * valid, > best
 i - internal, S stale
 Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i172.20.17.121	10.0.101.2		100	0 3	2000 3000 i
*>i10.0.0.0	10.0.101.2		100	0 3	100 1000 i
*>i172.5.23.0/24	10.0.101.2		100	0 3 4	60 4378 i

Table 28 describes the significant fields shown in the display.

Table 28 *show bgp regexp Field Descriptions*

Field	Description
BGP router identifier	BGP identifier for the local system.
local AS number	Autonomous system number for the local system.
Dampening enabled	Displayed if dampening has been enabled for the routes in this BGP routing table.
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
BGP scan interval	Interval (in seconds) between scans of the BGP table specified by the address family and subaddress family.

R3.3 Beta Draft—Cisco Confidential Information

Table 28 *show bgp regexp Field Descriptions (continued)*

Field	Description
Status codes	Status of the table entry. The status is displayed as a three-character field at the beginning of each line in the table. The first character may be (in order of precedence): S—Path is stale, indicating that a graceful restart is in progress with the peer from which the route was learned. s—Path is more specific than a locally sourced aggregate route and has been suppressed. *—Path is valid. The second character may be (in order of precedence): >—Path is the best path to use for that network. d—Path is dampened. h—Path is a history entry, representing a route that is currently withdrawn, but that is being maintained to preserve dampening information. Such routes should never be marked as valid. The third character may be: i—Path was learned by an internal BGP (iBGP) session.
Origin codes	Origin of the path. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Path originated from an Interior Gateway Protocol (IGP) and was advertised with a network or aggregate-address command. e—Path 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	IP address of a network entity.
Next Hop	IP address of the next system that is used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network.
Metric	Value of the interautonomous system metric, otherwise known as the Multi Exit Discriminator (MED) metric.
LocPrf	Local preference value. This is used to determine the preferred exit point from the local autonomous system. It is propagated throughout the local autonomous system.
Weight	Path weight. Weight is used in choosing the preferred path to a route. It is not advertised to any neighbor.
Path	Autonomous system path to the destination network. At the end of the path is the origin code for the path.

Related Commands

Command	Description
set default-afi	Sets the default Address Family Identifier (AFI) for the current session.
set default-safi	Sets the default Subaddress Family Identifier (SAFI) for the current session.

R3.3 Beta Draft – Cisco Confidential Information

Command	Description
show bgp	Displays entries in the BGP routing table.
show bgp route-policy	Displays BGP information about networks that match an outbound route policy.

R3.3 Beta Draft—Cisco Confidential Information

show bgp route-policy

To display Border Gateway Protocol (BGP) information about networks that match an outbound route policy, use the **show bgp route-policy** command in EXEC mode.

```
show bgp [ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
[vpnv4 unicast] [rd rd-address] | vrf {vrf-name | all} [ipv4 unicast]] route-policy
route-policy-name [count-only]
```

Syntax Description

ipv4	(Optional) Specifies IP Version 4 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
all	(Optional) For subaddress families, specifies prefixes for all subaddress families.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
all	(Optional) For address family, specifies prefixes for all address families.
vpnv4 unicast	(Optional) Specifies VPNv4 unicast address families.
rd rd-address	(Optional) Displays routes with a specific route distinguisher.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 unicast	(Optional) For VRF, specifies IPv4 unicast address families.
<i>route-policy-name</i>	Name of a route policy.
count-only	(Optional) Displays the number of prefixes or paths.

Defaults

If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The count-only keyword was added.
Release 3.3	The following keywords and arguments were added: vrf {vrf-name all} [ipv4 unicast] [vpnv4 unicast] [rd rd-address]

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.



Note

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

BGP contains a separate routing table for each address family and subaddress family combination that has been configured. The address family and subaddress family options specify the routing table to be examined. If the **all** keyword is specified for the address family or subaddress family, each matching routing table is examined.

A route policy must be configured to use this command. When the **show bgp route-policy** command is entered, routes in the specified BGP table are compared with the specified route policy, and all routes passed by the route policy are displayed.

If a pass clause is encountered while the route policy is being applied to the route and the route policy processing completes without hitting a drop clause, the route is displayed. The route is not displayed if a drop clause is encountered, if the route policy processing completes without hitting a pass clause, or if the specified route policy does not exist.

The information displayed does not reflect modifications the policy might make to the route. To display such modifications, use the **show bgp policy** command.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp route-policy** command in EXEC mode:

```
RP/0/RP0/CPU0:router# show bgp route-policy p1

BGP router identifier 172.20.1.1, local AS number 1820
BGP main routing table version 729
Dampening enabled
BGP scan interval 60 secs
Status codes: s suppressed, d damped, h history, * valid, > best
                i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
*  10.13.0.0/16    192.168.40.24             0 1878 704 701 200 ?
*  10.16.0.0/16    192.168.40.24             0 1878 704 701 i
```

Table 29 describes the significant fields shown in the display.

Table 29 *show bgp route-policy Field Descriptions*

Field	Description
BGP router identifier	BGP identifier for the local system.
local AS number	Autonomous system number for the local system.

R3.3 Beta Draft—Cisco Confidential Information

Table 29 *show bgp route-policy Field Descriptions (continued)*

Field	Description
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
Dampening enabled	Displayed if dampening is enabled for the routes in this BGP routing table.
BGP scan interval	Interval (in seconds) between scans of the BGP table specified by the address family and subaddress family.
Status codes	Status of the table entry. The status is displayed as a three-character field at the beginning of each line in the table. The first character may be (in order of precedence): S—Path is stale, indicating that a graceful restart is in progress with the peer from which the route was learned. s—Path is more specific than a locally sourced aggregate route and has been suppressed. *—Path is valid. The second character may be (in order of precedence): >—Path is the best path to use for that network. d—Path is dampened. h—Path is a history entry, representing a route that is currently withdrawn, but that is being maintained to preserve dampening information. Such routes should never be marked as valid. The third character may be: i—Path was learned by an internal BGP (iBGP) session.
Origin codes	Origin of the path. The origin code is displayed at the end of each line in the table. It can be one of the following values: i—Path originated from an Interior Gateway Protocol (IGP) and was advertised with a network or aggregate-address command. e—Path 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	IP prefix and prefix length for a network.
Next Hop	IP address of the next system that is used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network.
Metric	Value of the interautonomous system metric, otherwise known as the Multi Exit discriminator (MED) metric.
LocPrf	Local preference value. This is used to determine the preferred exit point from the local autonomous system. It is propagated throughout the local autonomous system.

R3.3 Beta Draft – Cisco Confidential Information**Table 29** *show bgp route-policy Field Descriptions (continued)*

Field	Description
Weight	Path weight. Weight is used in choosing the preferred path to a route. It is not advertised to any neighbor.
Path	Autonomous system path to the destination network. At the end of the path is the origin code for the path.

Related Commands

Command	Description
aggregate-address	Configures an aggregate entry in a BGP routing table.
network (BGP)	Specifies a local network that the BGP routing process should originate and advertise to its neighbors.
route-policy (BGP)	Applies a routing policy to updates advertised to or received from a BGP neighbor
route-policy	Configures a route policy.
set default-afi	Sets the default Address Family Identifier (AFI) for the current session.
set default-safi	Sets the default Subaddress Family Identifier (SAFI) for the current session.
show bgp policy	Displays advertisements under a proposed policy.

R3.3 Beta Draft—Cisco Confidential Information

show bgp session-group

To display information about the Border Gateway Protocol (BGP) configuration for session groups, use the **show bgp session-group** command in EXEC mode.

show bgp session-group *group-name* { **configuration** [**defaults**] [**nvgen**] | **inheritance** | **users** }

Syntax Description

<i>group-name</i>	Name of the session family group to display.
configuration	(Optional) Displays the effective configuration for the session group, including any inherited configuration.
defaults	(Optional) Displays all configuration, including default configuration.
nvgen	(Optional) Displays output in the form of the show running-config command.
	Note If the defaults keyword also is specified, the output is not suitable for cutting and pasting into a configuration session.
inheritance	(Optional) Displays the session groups from which this session group inherits configuration.
users	(Optional) Display the session groups, neighbor groups, and neighbors that inherit configuration from this session group.

Defaults

No default behavior or value

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show bgp session-group** command with the *group-name* **configuration** argument and keyword to display the effective configuration of a session group, including any configuration inherited from other session groups through application of the **use** command. The source for each configured command is also displayed.

Use the **defaults** keyword to display the value of all configuration, including default configuration. Use the **nvgen** keyword to display configuration in the form of the **show running-config** command output. Output in this form is suitable for cutting and pasting into a configuration session.

R3.3 Beta Draft—Cisco Confidential Information

Use the **show bgp session-group** command with the *group-name* **inheritance** argument and keyword to display the session groups from which the specified session group inherits configuration.

Use the **show bgp session-group** command with the *group-name* **users** argument and keyword to display the neighbors, neighbor groups, and session groups that inherit configuration from the specified session group.

Task ID	Task ID	Operations
	bgp	read

Examples

For the example shown here, the following configuration is used:

```
session-group group3
  advertisement-interval 5
  dmzlink-bw
  !
session-group group1
  use session-group group2
  update-source Loopback0
  !
session-group group2
  use session-group group3
  ebgp-multihop 2
```

The following example shows the **show bgp session-group** command with the **configuration** keyword:

```
RP/0/RP0/CPU0:router# show bgp session-group group1 configuration
```

```
session-group group1
  advertisement-interval 5[s:group2 s:group3]
  ebgp-multihop 2 [s:group2]
  update-source Loopback0 []
  dmzlink-bw [s:group2 s:group3]
```

The source of each command is shown to the right of the command. For example, **update-source** is configured directly on session group group1. The **dmzlink-bw** command is inherited from session group group2, which in turn inherits it from session group group3.

The following example shows the **show bgp session-group** command with the **users** keyword:

```
RP/0/RP0/CPU0:router# show bgp session-group group2 users
```

```
IPv4 Unicast:a:group1
```

The following example shows the **show bgp session-group** command with the **inheritance** keyword.

```
RP/0/RP0/CPU0:router# show bgp session-group group1 inheritance
```

```
Session:s:group2 s:group3
```

The command output shows that the session group group1 directly uses the group2 session group. The group2 session group uses the group3 session group.

Table 30 describes the significant fields shown in the display.

R3.3 Beta Draft – Cisco Confidential Information

Table 30 *show bgp session-group Field Descriptions*

Field	Description
[]	Configures the command directly on the specified session group.
s:	Indicates the name that follows is a session group.
a:	Indicates the name that follows is an address family group.
n:	Indicates the name that follows is a neighbor group.
[dflt]	Indicates the command is not explicitly configured or inherited, and the default value for the command is used. This field may be shown when the defaults keyword is specified.
<not set>	Indicates that the default is for the command to be disabled. This field may be shown when the defaults keyword is specified.

Related Commands

Command	Description
session-group	Configures a BGP session group.
show bgp neighbor-group	Displays information about the BGP configuration for neighbor groups.
show bgp neighbors	Displays information about BGP connections to neighbors.

R3.3 Beta Draft – Cisco Confidential Information

show bgp summary

To display the status of all Border Gateway Protocol (BGP) connections, use the **show bgp summary** command in EXEC mode.

```
show bgp [ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
vpnv4 unicast | vrf {vrf-name | all} [ipv4 unicast]] summary
```

Syntax Description	
ipv4	(Optional) Specifies IP Version 4 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
all	(Optional) For subaddress families, specifies prefixes for all subaddress families.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
all	(Optional) For address family, specifies prefixes for all address families.
vpnv4 unicast	(Optional) Specifies VPNv4 unicast address families.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 unicast	(Optional) For VRF, specifies IPv4 unicast address families.

Defaults If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	The following keywords and arguments were added: vrf {vrf-name all} [ipv4 unicast] vpnv4 unicast

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information



Note

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

Use the **show bgp summary** command to display a summary of the neighbors for which the specified address family and subaddress family are enabled. If the neighbor does not have the specified address family and subaddress family enabled, it is not included in the output of the **show** command. If the **all** keyword is specified for the address family or subaddress family, a summary for each combination of address family and subaddress family is displayed in turn.

The table versions shown in the output (RcvTblVer, bRIB/RIB, SendTblVer, and TblVer) are specific to the specified address family and subaddress family. All other information is global.

The table versions provide an indication of whether BGP is up to date with all work for the specified address family and subaddress family.

- bRIB/RIB < RcvTblVer—Some received routes have not yet been considered for installation in the global routing table.
- TblVer < SendTblVer—Some received routes have been installed in the global routing table but have not yet been considered for advertisement to this neighbor.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp summary** command:

```
RP/0/RP0/CPU0:router# show bgp summary
```

```
BGP router identifier 10.140.140.1, local AS number 140
BGP main routing table version 1
BGP scan interval 60 secs
BGP is operating in STANDALONE mode.
```

Process Speaker	RecvTblVer 1	bRIB/RIB 1	SendTblVer 1						
Neighbor	Spr	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	St/PfxRcd
172.20.1.1	0	1	0	0	0	0	0	00:00:00	Idle
172.23.1.1	0	2	0	0	0	0	0	00:00:00	Idle
172.21.1.1	0	140	0	0	0	0	0	00:00:00	Active
172.22.1.1	0	5	0	0	0	0	0	00:00:00	Idle
10.30.30.1	0	40	0	321	0	0	0	00:00:00	Active

Table 31 describes the significant fields shown in the display.

R3.3 Beta Draft—Cisco Confidential Information**Table 31** *show bgp summary Field Descriptions*

Field	Description
BGP router identifier	IP address of the router.
local AS number	Autonomous system number set by the router bgp command.
BGP main routing table version	Last version of the BGP database that was injected into the main routing table.
Dampening enabled	Displayed if dampening has been enabled for the routes in this BGP routing table.
BGP Scan interval	Interval (in seconds) between scans of the BGP table specified by the address family and subaddress family.
BGP is operating in	Specifies BGP is operating in standalone mode.
Process	BGP process.
RecvTblVer	Last version used in the BGP database for received routes.
bRIB/RIB	Last version of the local BGP database that was injected into the main routing table.
SendTblVer	Latest version of the local BGP database that is ready to be advertised to neighbors.
Some configured eBGP neighbors do not have any policy	Some external neighbors exist that do not have both an inbound and outbound policy configured for every address family, using the route-policy (BGP) command. In this case, no prefixes are accepted and advertised to those neighbors.
Neighbor	IP address of a neighbor.
Spr	Speaker process that is responsible for the neighbor. Always 0.
AS	Autonomous system.
MsgRcvd	Number of BGP messages received from a neighbor.
MsgSent	Number of BGP messages sent to a neighbor.
TblVer	Last version of the BGP database that was sent to a neighbor.
InQ	Number of messages from a neighbor waiting to be processed.
OutQ	Number of messages waiting to be sent to a neighbor.

R3.3 Beta Draft – Cisco Confidential Information

Table 31 *show bgp summary Field Descriptions (continued)*

Field	Description
Up/Down	Length of time in (hh:mm:ss) that the BGP session has been in Established state, or the time since the session left Established state, if it is not established.
St/PfxRcd	If the BGP session is not established, the current state of the session. If the session is established, the number of prefixes the router has received from the neighbor. If the number of prefixes received exceeds the maximum allowed (as set by the maximum-prefix command), “(PfxRcd)” appears. If the connection has been shut down using the shutdown command, “(Admin)” appears. If the neighbor is external and it does not have an inbound and outbound policy configured for every address family, an exclamation mark (!) is inserted at the end of the state when using the route-policy (BGP) command. If the connection has been shut down due to out of memory (OOM), “(OOM)” appears.

Related Commands

Command	Description
route-policy (BGP)	Applies a routing policy to updates advertised to or received from a BGP neighbor.
set default-afi	Sets the default Address Family Identifier (AFI) for the current session.
set default-safi	Sets the default Subaddress Family Identifier (SAFI) for the current session.

R3.3 Beta Draft—Cisco Confidential Information

show bgp truncated-communities

To display routes in the Border Gateway Protocol (BGP) routing table for which inbound policy or aggregation has exceeded the maximum number of communities that may be attached, use the **show bgp truncated-communities** command in EXEC mode.

```
show bgp [ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
[vpn4 unicast] [rd rd-address] | vrf {vrf-name | all} [ipv4 unicast]] truncated-communities
[count-only]
```

Syntax Description	
ipv4	(Optional) Specifies IP Version 4 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
all	(Optional) For subaddress families, specifies prefixes for all subaddress families.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
all	(Optional) For address family, specifies prefixes for all address families.
vpn4 unicast	(Optional) Specifies VPNv4 unicast address families.
rd rd-address	(Optional) Displays routes with a specific route distinguisher.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 unicast	(Optional) For VRF, specifies IPv4 unicast address families.
count-only	(Optional) Displays the number of prefixes or paths.

Defaults If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The count-only keyword was added.
	Release 3.3	The following keywords and arguments were added: vrf {vrf-name all} [ipv4 unicast] [vpn4 unicast] [rd rd-address]

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.



Note

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

BGP contains a separate routing table for each address family and subaddress family combination that has been configured. The address family and subaddress family options specify the routing table to be examined. If the **all** keyword is specified for the address family or subaddress family, each matching routing table is examined.

Use the **show bgp truncated-communities** command to display those routes in the specified BGP routing table in which the buffers used to store communities or extended communities have overflowed. An overflow occurs if an attempt is made to associate more communities or extended communities with the route than fits in a BGP update message. This can happen due to modification of communities or extended communities during aggregation or when inbound policy is applied.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp truncated-communities** command:

```
RP/0/RP0/CPU0:router# show bgp truncated-communities

BGP router identifier 172.20.1.1, local AS number 1820
BGP main routing table version 3042
BGP scan interval 60 secs
Status codes: s suppressed, d damped, h history, * valid, > best
                i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
*  10.13.0.0/16    192.168.40.24                0 1878 704 701 200 ?
*> 10.16.0.0/16    192.168.40.24                0 1878 704 701 i
```

Table 32 describes the significant fields shown in the display.

Table 32 *show bgp truncated-communities Field Descriptions*

Field	Description
BGP router identifier	BGP Identifier for the local system.
local AS number	Autonomous system number for the local system.
BGP main routing table version	Last version of the BGP database that was installed into the main routing table.
Dampening enabled	Displayed if dampening is enabled for the routes in this BGP routing table.

R3.3 Beta Draft—Cisco Confidential Information**Table 32** *show bgp truncated-communities Field Descriptions (continued)*

Field	Description
BGP scan interval	Interval (in seconds) between scans of the BGP table specified by the address family and subaddress family.
Status codes	Status of the table entry. The status is displayed as a three-character field at the beginning of each line in the table. The first character may be (in order of precedence): S—Path is stale, indicating that a graceful restart is in progress with the peer from which the route was learned. s—Path is more specific than a locally sourced aggregate route and has been suppressed. *—Path is valid. The second character may be (in order of precedence): >—Path is the best path to use for that network. d—Path is dampened. h—Path is a history entry, representing a route that is currently withdrawn, but that is being maintained to preserve dampening information. Such routes should never be marked as valid. The third character may be: i—Path was learned by an internal BGP (iBGP) session.
Origin codes	Origin of the path. The origin code is displayed at the end of each line in the table. It can be one of the following values: i—Path originated from an Interior Gateway Protocol (IGP) and was advertised with a network or aggregate-address command. e—Path 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	IP prefix and prefix length for a network.
Next Hop	IP address of the next system that is used when a packet is forwarded to the destination network. An entry of 0.0.0.0 indicates that the router has a non-BGP route to this network.
Metric	Value of the interautonomous system metric, otherwise known as the Multi Exit Discriminator (MED) metric.
LocPrf	Local preference value. This is used to determine the preferred exit point from the local autonomous system. It is propagated throughout the local autonomous system.
Weight	Path weight. Weight is used in choosing the preferred path to a route. It is not advertised to any neighbor.
Path	Autonomous system path to the destination network. At the end of the path is the origin code for the path.

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	aggregate-address	Creates an aggregate entry in a BGP routing table.
	network (BGP)	Specifies a local network that the BGP routing process should originate and advertise to its neighbors.
	route-policy (BGP)	Applies a routing policy to updates advertised to or received from a BGP neighbor.
	set default-afi	Sets the default Address Family Identifier (AFI) for the current session.
	set default-safi	Sets the default Subaddress Family Identifier (SAFI) for the current session.
	show bgp	Displays entries in the BGP routing table.

R3.3 Beta Draft—Cisco Confidential Information

show bgp update-group

To display Border Gateway Protocol (BGP) information for update groups, use the **show bgp update-group** command in EXEC mode.

```
show bgp [ipv4 {unicast | multicast | all} | ipv6 {unicast | all} | all {unicast | multicast | all} |
vpnv4 unicast | vrf {vrf-name | all} [ipv4 unicast]] update-group [neighbor ip-address |
process-id.index [summary | performance-statistics]]
```

Syntax Description	
ipv4	(Optional) Specifies IP Version 4 update groups.
unicast	(Optional) Specifies unicast update groups.
multicast	(Optional) Specifies multicast update groups.
all	(Optional) Displays both unicast and multicast update groups.
ipv6	(Optional) Specifies IP Version 6 update groups.
all	(Optional) Displays both IP Version 4 and IP Version 6 update groups.
vpnv4 unicast	(Optional) Specifies VPNv4 unicast address families.
rd <i>rd-address</i>	(Optional) Displays routes with a specific route distinguisher.
vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of a VRF.
all	(Optional) For VRF, specifies all VRFs.
ipv4 unicast	(Optional) For VRF, specifies IPv4 unicast address families.
neighbor <i>ip-address</i>	(Optional) Specifies information on an update group for a specific neighbor.
<i>process-id.index</i>	(Optional) Update group index. Process ID range is 0 to 254. Index range is 0 to 4294967295.
	Note The <i>process id.index</i> argument is specified as follows: process ID (dot) index. In standalone mode, the process ID is always 0.
summary	(Optional) Specifies summary of update group members.
performance-statistics	(Optional) Specifies performance information about the updates generated for the update group.

Defaults If no address family or subaddress family is specified, the default address family and subaddress family specified using the **set default-afi** and **set default-safi** commands are used.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Release	Modification
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	The following keywords and arguments were added: • vrf { <i>vrf-name</i> all } [ipv4 unicast] • [vpnv4 unicast]

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.



Note

The **set default-afi** command is used to specify the default address family for the session, and the **set default-safi** command is used to specify the default subaddress family for the session. See the *Cisco IOS XR System Management Command Reference* for detailed information and syntax for the **set default-afi** and **set default-safi** commands. If you do not specify a default address family, the default address family is IPv4. If you do not specify a default subaddress family, the default subaddress family is unicast.

Every BGP neighbor is automatically assigned to an update group for each address family that is enabled on the neighbor. Neighbors that have similar outbound policy, such that they are sent the same updates, are placed in the same update group.

Use the **show bgp update-group** command to display the update groups and a list of the neighbors that belong to the update group.

Use the **show bgp update-group neighbor** command to display details about the update group to which a neighbor belongs for the specified address family.

Use the **summary** keyword to display a summary of the neighbors belonging to the specified update group. The display format is the same as for the **show bgp summary** command.

Use the **performance-statistics** keyword to display information about the number of prefixes processed and the time taken to generate updates for the specified update group.



Note

Update group indexes are not necessarily persistent over a process restart. If a BGP process restarts, the index of the update group to which a particular neighbor is assigned may be different, though the set of neighbors belonging to the update group is the same.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp update-group** command:

```
RP/0/RP0/CPU0:router# show bgp update-group
```

```
Update group for IPv4 Unicast, index 0.1:
```

```
Attributes:
```

```
Internal
```

```
Common admin
```

R3.3 Beta Draft—Cisco Confidential Information

```

Send communities
Minimum advertisement interval:5
Messages formatted:0, replicated:0
Neighbors in this update group:
172.20.1.1

```

Table 33 describes the significant fields shown in the display.

Table 33 *show bgp update-group Field Descriptions*

Field	Description
Update group for	Address family to which updates in this update group apply.
index	Update group index.
Attributes	Attributes common to all members of the update group.
Unsuppress map	Unsuppress route map used to selectively unsuppress more specific routes of locally generated aggregates for members of this update group.
Outbound policy	Route policy applied to outbound updates generated for members of this update group.
Internal	Members of the update group are internal peers.
ORF Receive enabled	Members of this update group are capable of receiving an outbound route filter.
Route Reflector Client	Local system is acting as a route reflector for members of this update group.
Remove private AS numbers	Members of this update group have private AS numbers stripped from outbound updates.
Next-hop-self enabled	Next hop calculation for the members of this update group is disabled.
Directly connected IPv6 EBGp	Members of this update group are directly connected external BGP IPv6-based peers.
Minimum advertisement interval	Minimum advertisement interval for members of this update group.
Configured Local AS	Local autonomous system (AS) used for members of this update group.
Common admin	Peers in this update group are under common administration (internal or confederation peers).
Send communities	Communities are sent to neighbors in this update group.
Send extended communities	Extended communities is sent to neighbors in this update group.
replicated	Number of update messages replicated for this update group.
Messages formatted	Number of update messages generated for this update group.
Neighbors in this update group	List of neighbors that use this update group for the given address family.

The following is sample output from the **show bgp update-group** command with the **ipv4**, **unicast**, and **summary** keywords and the *process id.index* argument:

```

RP/0/RP0/CPU0:router# show bgp ipv4 unicast update-group 0.1 summary

BGP router identifier 10.140.140.1, local AS number 1
BGP main routing table version 1

```

```
show bgp update-group
```

R3.3 Beta Draft—Cisco Confidential Information

```
BGP scan interval 60 secs
BGP is operating in STANDALONE mode.
```

```
Process          RecvTblVer    bRIB/RIB    SendTblVer
  Speaker              1              1              1

Neighbor          Spr      AS  MsgRcvd  MsgSent    TblVer  InQ  OutQ  Up/Down  St/PfxRcd
172.25.11.8        0        1        0        0          0     0    0  00:00:00  Idle
```

Table 34 describes the significant fields shown in the display.

Table 34 *show bgp ipv4 unicast update-group Field Descriptions*

Field	Description
BGP router identifier	IP address of the router.
local AS number	Autonomous system number set by the router bgp command.
BGP main routing table version	Last version of the BGP database that was injected into the main routing table.
Dampening enabled	Displayed if dampening has been enabled for the routes in this BGP routing table.
BGP scan interval	Interval (in seconds) between scans of the BGP table specified by the address family and subaddress family.
BGP is operating in	BGP is operating in standalone mode.
Process	BGP process.
RecvTblVer	Last version used in the BGP database for received routes.
bRIB/RIB	Last version of the local BGP database that was injected into the main routing table.
SendTblVer	Latest version of the local BGP database that is ready to be advertised to neighbors.
Some configured eBGP neighbors do not have any policy	Some external neighbors that exist do not have both an inbound and outbound policy configured for every address family, using the route-policy (BGP) command. In this case, no prefixes are accepted or advertised to those neighbors.
Neighbor	IP address of a neighbor.
Spr	Speaker process that is responsible for the neighbor. Always 0.
AS	Autonomous system.
MsgRcvd	Number of BGP messages received from a neighbor.
MsgSent	Number of BGP messages sent to a neighbor.
TblVer	Last version of the BGP database that was sent to a neighbor.
InQ	Number of messages from a neighbor waiting to be processed.
OutQ	Number of messages waiting to be sent to a neighbor.

R3.3 Beta Draft – Cisco Confidential Information

Table 34 *show bgp ipv4 unicast update-group Field Descriptions (continued)*

Field	Description
Up/Down	Length of time (in hh:mm:s) that the BGP session has been in Established state, or the time since the session left Established state, if it is not established.
St/PfxRcd	If the BGP session is not established, the current state of the session. If the session is established, the number of prefixes the router has received from the neighbor. If the number of prefixes received exceeds the maximum allowed (as set by the maximum-prefix command), “(PfxRcd)” appears. If the connection has been shut down using the shutdown command, “(Admin)” appears. If the neighbor is external and it does not have an inbound and outbound policy configured for every address family, an exclamation mark (!) is inserted at the end of the state when using the route-policy (BGP) command.

Related Commands

Command	Description
maximum-prefix (BGP)	Limits the number of prefixes that can be received from a neighbor.
route-policy (BGP)	Applies a routing policy to updates advertised to or received from a BGP neighbor.
set default-afi	Sets the default Address Family Identifier (AFI) for the current session.
set default-safi	Sets the default Subaddress Family Identifier (SAFI) for the current session.
show bgp summary	Displays the status of all BGP connections.
shutdown (BGP)	Disables a neighbor without removing its configuration.

R3.3 Beta Draft—Cisco Confidential Information

show bgp vrf imported-routes

To display Border Gateway Protocol (BGP) information for routes imported into specified VPN routing and forwarding (VRF) instances, use the **show bgp vrf imported-routes** command in EXEC mode.

```
show bgp vrf {vrf-name | all} [ipv4 unicast] imported-routes [vrf source-vrf-name] [neighbor neighbor-address]
```

Syntax Description

<i>vrf-name</i>	Displays imported routes for a specific VRF.
all	Displays imported routes for all VRFs.
ipv4 unicast	(Optional) Specifies IP Version 4 unicast imported routes.
vrf <i>source-vrf-name</i>	(Optional) Displays routes imported into the source VRF.
neighbor <i>neighbor-address</i>	(Optional) Displays preview advertisements for a specified neighbor.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
bgp	read

Examples

The following is sample output from the **show bgp vrf imported-routes** command:

```
RP/0/RP0/CPU0:router# show bgp vrf vrf-1 imported-routes
```

```
BGP VRF vrf-1, state: Active
BGP Route Distinguisher: 10.1.0.1:0
BGP router identifier 10.1.0.1, local AS number 100 BGP generic scan interval 60 secs BGP
table state: Active BGP main routing table version 3000095 BGP scan interval 60 secs
Status codes: s suppressed, d damped, h history, * valid, > best
                i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

R3.3 Beta Draft—Cisco Confidential Information

Network	Neighbor	Route Distinguisher	Source VRF
*>i1.0.1.0/30	10.0.101.1	2.2.2.2:1001	default
*>i1.0.1.4/30	10.0.101.1	2.2.2.2:1002	default
*>i1.0.1.8/30	10.0.101.1	2.2.2.2:1003	default
*>i1.0.1.12/30	10.0.101.1	2.2.2.2:1004	default
*>i1.0.1.16/30	10.0.101.1	2.2.2.2:1005	default
*>i1.0.1.20/30	10.0.101.1	2.2.2.2:1006	default
*>i1.0.1.24/30	10.0.101.1	2.2.2.2:1007	default
*>i1.0.1.28/30	10.0.101.1	2.2.2.2:1008	default
*>i1.0.1.32/30	10.0.101.1	2.2.2.2:1009	default

R3.3 Beta Draft—Cisco Confidential Information

show protocols (BGP)

To display information about the Border Gateway Protocol (BGP) instances running on the router, use the **show protocols** command in EXEC mode and specify either the **bgp** or **all** keyword.

```
show protocols [ipv4 | ipv6] [all | protocol]
```

Syntax Description

ipv4 ipv6	(Optional) Specifies an address family. The options are ipv4 or ipv6 .
all	(Optional) Specifies all protocols for a given address family.
<i>protocol</i>	(Optional) Specifies a routing protocol. - For the IPv4 address family, the options are bgp, isis, and ospf. - For the IPv6 address family, the options are bgp, isis, and ospfv3.

Defaults

Default is IPv4.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show protocols** command to get information about the protocols running on the router and to quickly determine which protocols are active. The command is designed to summarize the important characteristics of the running protocol, and command output varies depending on the specific protocol selected. For BGP, the command output lists the protocol ID, peers with elapsed time since last reset, and miscellaneous information, such as external and internal local distances and sourced routes.

Task ID

Task ID	Operations
bgp	read
rib	read

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows the display for the **show protocols** command using the **bgp** keyword:

```
RP/0/RP0/CPU0:router# show protocols bgp

Routing Protocol "BGP 40"

Address Family IPv4 Unicast:
  Distance: external 20 internal 200 local 200
  Sourced Networks:
    10.100.0.0/16 backdoor
    10.100.1.0/24
    10.100.2.0/24
  Routing Information Sources:
    Neighbor          State/Last update received
    10.5.0.2           Idle
    10.9.0.3           Idle
```

Table 35 describes the significant fields shown in the display.

Table 35 *show protocols (BGP) Field Descriptions*

Field	Description
Routing Protocol:	Identifies BGP as the running protocol and displays the BGP AS number.
Address Family	Specifies the address family. This can be IPv4 Unicast, IPv4 Multicast, or IPv6 Unicast.
Distance: external	Specifies the distance BGP sets when installing eBGP routes into the RIB. eBGP routes are routes received from eBGP peers. The RIB uses the distance as a tiebreaker when several protocols install a route for the same prefix.
Distance: internal	Specifies the distance BGP sets for routes received from iBGP peers.
Distance: local	Specifies the distance BGP sets for locally generated aggregates and backdoor routes.
Sourced Networks	List of locally sourced networks. These are networks sourced using the network command.
Routing information Sources	List of configured BGP neighbors.
Neighbor	Address of a BGP neighbor.
State/Last update received	State of each neighbor and the time since the last update was received from the neighbor if it is established.

R3.3 Beta Draft—Cisco Confidential Information**shutdown (BGP)**

To disable a neighbor without removing its configuration, use the **shutdown** command in an appropriate configuration mode. To re-enable the neighbor and reestablish a Border Gateway Protocol (BGP) session, use the **no** form of this command.

shutdown [disable]

no shutdown

Syntax Description

disable	(Optional) Overrides the value of a shutdown command inherited from a neighbor group or session group.

Defaults

Neighbors are not shutdown.

Command Modes

Neighbor configuration
VRF neighbor configuration
Neighbor group configuration
Session group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in the VRF neighbor configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **shutdown** command to terminate any active session for the specified neighbor and remove all associated routing information. Use of the **shutdown** command with a neighbor group or session group may suddenly terminate a large number of BGP neighbor sessions because all neighbors using the neighbor group or session group may be affected.

Use the **show bgp summary** command to display a summary of BGP neighbors. Neighbors that are idle due to the **shutdown** command are displayed with the “Idle (Admin)” state.

If this command is configured for a neighbor group or session group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	bgp	read, write

Examples

The following example shows that any active session for neighbor 192.168.40.24 is disabled:

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# neighbor 192.168.40.24
RP/0/RP0/CPU0:router(config-bgp-nbr)# shutdown
RP/0/RP0/CPU0:router(config-bgp-nbr)# exit
```

In the following example, the session remains active for neighbor 192.168.40.24 because the inherited **shutdown** command has been overridden:

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# session-group group1
RP/0/RP0/CPU0:router(config-bgp-sngrp)# shutdown
RP/0/RP0/CPU0:router(config-bgp-sngrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 192.168.40.24
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# use session-group group1
RP/0/RP0/CPU0:router(config-bgp-nbr)# shutdown disable
RP/0/RP0/CPU0:router(config-bgp-nbr)# exit
```

Related Commands	Command	Description
	neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
	session-group	Creates a session group and enters session group configuration mode.
	show bgp summary	Displays the status of all BGP connections.

R3.3 Beta Draft—Cisco Confidential Information

socket receive-buffer-size

To set the size of the receive buffers for all Border Gateway Protocol (BGP) neighbors, use the **socket receive-buffer-size** command in an appropriate configuration mode. To set the size of the receive buffers to the default size, use the **no** form of this command.

socket receive-buffer-size *socket-size* [*bgp-size*]

no socket receive-buffer-size

Syntax Description

<i>socket-size</i>	Size (in bytes) of the receive-side socket buffers. Range is 512 to 131072.
<i>bgp-size</i>	(Optional) Size (in bytes) of the receive buffers in BGP. Range is 512 to 131072.

Defaults

socket-size: 32,768 bytes
bgp-size: 4,032 bytes

Command Modes

Router configuration
 VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **socket receive-buffer-size** command to increase the buffer size when receiving updates from a neighbor. Using larger buffers can improve convergence time because the software can process more packets simultaneously. However, allocating larger buffers uses more memory on your router.

**Note**

Increasing the socket buffer size uses more memory only when more messages are waiting to be processed by the software. In contrast, increasing the BGP buffer size uses extra memory indefinitely.

Use the **receive-buffer-size** command on individual neighbors to change the values set by the **socket receive-buffer-size** command.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	bgp	read, write

Examples The following example shows how to set the receive buffer sizes for all neighbors to 65,536 bytes for the socket buffer and 8192 bytes for the BGP buffer:

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# socket receive-buffer-size 65536 8192
```

Related Commands	Command	Description
	receive-buffer-size	Sets the size of the receive buffers for a BGP neighbor.
	socket send-buffer-size	Sets the size of the send buffers for all BGP neighbors.

R3.3 Beta Draft—Cisco Confidential Information

socket send-buffer-size

To set the size of the send buffers for all Border Gateway Protocol (BGP) neighbors, use the **socket send-buffer-size** command in an appropriate configuration mode. To set the size of the send buffers to the default size, use the **no** form of this command.

socket send-buffer-size *socket-size* [*bgp-size*]

no socket send-buffer-size

Syntax Description	<i>socket-size</i>	Size (in bytes) of the send-side socket buffers.
	<i>bgp-size</i>	(Optional) Size (in bytes) of the send buffers in BGP.

Defaults	<i>socket-size</i> : 4096 bytes
	<i>bgp-size</i> : 4096 bytes

Command Modes	Router configuration
	VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in the VRF configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the socket send-buffer-size command to increase the buffer size when sending updates to neighbors. Using larger buffers can improve convergence time because the software can process more packets simultaneously. However, allocating larger buffers uses more memory on your router.

**Note**

Increasing the socket buffer size uses more memory only when more messages are waiting to be sent by the software. In contrast, increasing the BGP buffer size uses extra memory indefinitely.

Use the **send-buffer-size** command on individual neighbors to change the values set by the **socket send-buffer-size** command.

Task ID	Task ID	Operations
	bgp	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to set the send buffer sizes for all neighbors to 8192 bytes for the socket buffer and the BGP buffer:

```
RP/0/RP0/CPU0:router(config)# router bgp 1  
RP/0/RP0/CPU0:router(config-bgp)# socket send-buffer-size 8192 8192
```

Related Commands

Command	Description
send-buffer-size	Sets the size of the send buffers for a BGP neighbor.
socket receive-buffer-size	Sets the size of the receive buffers for all BGP neighbors.

R3.3 Beta Draft—Cisco Confidential Information

soft-reconfiguration inbound

To configure the software to store updates received from a neighbor, use the **soft-reconfiguration inbound** command in an appropriate configuration mode. To disable storing received updates, use the **no** form of this command.

soft-reconfiguration inbound [**always** | **disable**]

no soft-reconfiguration inbound

Syntax Description	always	(Optional) Always performs a soft inbound clear using stored updates, even if the neighbor supports the route refresh capability.
	disable	(Optional) Overrides configuration for this command that may be inherited from a neighbor group or address family group.

Defaults Soft reconfiguration is not enabled.

Command Modes

- IPv4 address family group configuration
- IPv6 address family group configuration
- VPNv4 address family group configuration
- IPv4 neighbor address family configuration
- VPNv4 neighbor address family configuration
- VRF IPv4 neighbor address family configuration
- IPv4 neighbor group address family configuration
- IPv6 neighbor group address family configuration
- VPNv4 neighbor group address family configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in the following configuration modes: • VPNv4 address family group • VPNv4 neighbor address family • VRF IPv4 neighbor address family • VPNv4 neighbor group address family

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information

To filter or modify some of the updates received from a neighbor, you configure an inbound policy using the **route-policy (BGP)** command or **prefix-list** command. Configuring soft reconfiguration inbound causes the software to store the original unmodified route besides a route that is modified or filtered. This allows a “soft clear” to be performed after the inbound policy is changed. To perform a soft clear, use the **clear bgp soft** command with the **in** keyword specified. The unmodified routes are then passed through the new policy and installed in the BGP table.



Note

The **bgp auto-policy-soft-reset** is enabled by default. A soft clear is done automatically when the inbound policy configured with the **route-policy (BGP)** command is changed. This behavior can be changed by disabling the auto-policy-soft-reset using the **bgp auto-policy-soft-reset disable** command.

If the neighbor supports the route refresh capability, then the original routes are not stored because they can be retrieved from the neighbor through a route refresh request. However, if the **always** keyword is specified, the original routes are stored even when the neighbor supports the route refresh capability.

If the **soft-reconfiguration inbound** command is not configured and the neighbor does not support the route refresh capability, then an inbound soft clear is not possible. In that case, the only way to rerun the inbound policy is to use the **clear bgp ip-address** command to reset the neighbor BGP session.



Note

If there is an existing BGP session with a neighbor that does not support the route refresh capability, the session is terminated and a new one is initiated.



Note

The extra routes stored as a result of configuring this command use more memory on the router.

If you configure this command for a neighbor group or neighbor address family group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows inbound soft reconfiguration enabled for IP Version 4 (IPv4) unicast routes received from neighbor 10.108.1.1. The software stores all routes received in their unmodified form so that when an inbound soft clear is performed later, the stored information can then be used to generate a new set of modified routes.

```
RP/0/RP0/CPU0:router(config)# router bgp 100
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.108.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 100
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# soft-reconfiguration inbound
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# exit
```

The following example shows inbound soft reconfiguration disabled for neighbor 10.108.1.1, preventing this feature from being automatically inherited by address family group1:

```
RP/0/RP0/CPU0:router(config)# router bgp 100
RP/0/RP0/CPU0:router(config-bgp)# af-group group1 address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-afgrp)# soft-reconfiguration inbound
```

R3.3 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config-bgp-afgrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.108.1.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 100
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 multicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# use af-group group1
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# soft-reconfiguration inbound disable
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# exit
```

Related Commands

Command	Description
af-group	Creates an address family group for BGP neighbors and enters address family group configuration mode.
bgp bestpath as-path ignore	Enables an automatic soft reset of BGP peers when their configured route policy is modified.
clear bgp	Resets a BGP connection using a soft or hard reset.
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
route-policy (BGP)	Applies a routing policy to updates advertised to or received from a BGP neighbor.
rd	Applies a prefix list to filter updates received from a neighbor

R3.3 Beta Draft—Cisco Confidential Information

table-policy

To apply a routing policy to routes being installed into the routing table, use the **table-policy** command in an appropriate configuration mode. To disable applying a routing policy when installing routes into the routing table, use the **no** form of this command.

table-policy *policy-name*

no table-policy

Syntax Description

<i>policy-name</i>	Name of the routing policy to apply.

Defaults

No policy is applied when routes are installed into the routing table.

Command Modes

IPv4 address family configuration
IPv6 address family configuration
VRF IPv4 address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in the VRF IPv4 address family configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.



Note

Table policy provides users with the ability to drop routes from the RIB based on match criteria. This feature should be used with caution as it can easily create a routing ‘black-hole’ where BGP advertises routes to neighbors that BGP does not install in its global routing table but in the forwarding table.

Use the **table-policy** command to modify route attributes as the routes are installed into the routing table by Border Gateway Protocol (BGP). Commonly, it is used to set the traffic index attribute.

Task ID

Task ID	Operations
bgp	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to apply the set-traffic-index policy to IPv4 unicast routes being installed into the routing table:

```
RP/0/RP0/CPU0:router(config)# router bgp 1  
RP/0/RP0/CPU0:router(config-bgp)# address-family ipv4 unicast  
RP/0/RP0/CPU0:router(config-bgp-af)# table-policy set-traffic-index
```

Related Commands

Command	Description
route-policy (RPL)	Defines a route policy and enters route policy configuration mode.

R3.3 Beta Draft—Cisco Confidential Information

timers (BGP)

To set the timers for a specific Border Gateway Protocol (BGP) neighbor, use the **timers** command in an appropriate configuration mode. To set the timers to the default values, use the **no** form of this command.

timers *keepalive hold-time*

no timers

Syntax Description	<i>keepalive</i>	Frequency (in seconds) with which the software sends keepalive messages to a neighbor. Range is 0 to 4294967295.
	<i>hold-time</i>	Interval (in seconds) after not receiving a keepalive message from the neighbor that the software terminates the BGP session for the neighbor. Values are 0 or a number in the range from 3 to 4294967295.

Defaults

keepalive: 60 seconds

hold-time: 180 seconds

Use the **timers bgp** command to override the default values.

Command Modes

Neighbor configuration
VRF neighbor configuration
Neighbor group configuration
Session group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF neighbor configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The timers actually used in connection with the neighbor may not be the same as those configured with this command. The actual timers are negotiated with the neighbor when establishing the session. The negotiated hold time is the minimum of the configured time and the hold time received from the neighbor. If the negotiated hold time is 0, keepalives are disabled.

The configured value for the keepalive must not exceed one-third of the negotiated hold time. If it does, a value of one-third of the negotiated hold time is used.

R3.3 Beta Draft—Cisco Confidential Information

If this command is configured for a neighbor group or neighbor address family group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

Task ID	Task ID	Operations
	bgp	read, write

Examples

The following example shows how to change the keepalive timer to 70 seconds and the hold-time timer to 210 seconds for the BGP peer 192.168.40.24:

```
RP/0/RP0/CPU0:router(config)# router bgp 109
RP/0/RP0/CPU0:router(config-bgp)# neighbor 192.168.40.24
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# timers 70 210
RP/0/RP0/CPU0:router(config-bgp-nbr)# exit
```

Related Commands	Command	Description
	af-group	Creates an address family group for BGP neighbors and enters address family group configuration mode.
	neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
	session-group	Creates a session group and enters session group configuration mode.
	timers bgp	Adjusts BGP network timers for all BGP neighbors.

R3.3 Beta Draft—Cisco Confidential Information

timers bgp

To change the default timer values for Border Gateway Protocol (BGP) neighbors, use the **timers bgp** command in an appropriate configuration mode. To set the default timers to the default values, use the **no** form of this command.

timers bgp *keepalive hold-time*

no timers bgp

Syntax Description	<i>keepalive</i>	Frequency (in seconds) with which the software sends keepalive messages to the neighbor. Range is 0 to 4294967295.
	<i>hold-time</i>	Interval (in seconds) after not receiving a keepalive message from the neighbor that the software terminates the BGP session for the neighbor. Values are 0 or a number in the range from 3 to 4294967295.

Defaults	<i>keepalive</i> : 60 seconds <i>hold-time</i> : 180 seconds

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in VRF configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **timers bgp** command to adjust the default timer times used by all BGP neighbors. The values can be overridden on particular neighbors using the **timers** command in the neighbor configuration mode.

The timers actually used in connection with the neighbor may not be the same as those configured with this command. The actual timers are negotiated with the neighbor when establishing the session. The negotiated hold time is the minimum of the configured time and the hold time received from the neighbor. If the negotiated hold time is 0, keepalives are disabled.

The configured value for the keepalive must not exceed one-third of the negotiated hold time. If it does, a value of one-third of the negotiated hold time is used.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	bgp	read, write

Examples The following example shows how to configure a default keepalive time of 30 seconds and a default hold time of 90 seconds:

```
RP/0/RP0/CPU0:router(config)# router bgp 1  
RP/0/RP0/CPU0:router(config-bgp)# timers bgp 30 90
```

Related Commands	Command	Description
	timers (BGP)	Adjusts BGP network timers for a BGP neighbor.

R3.3 Beta Draft—Cisco Confidential Information

ttl-security

To configure a router to check the time-to-live (TTL) field in incoming IP packets for the specified external Border Gateway Protocol (eBGP) peer, use the **ttl-security** command in an appropriate configuration mode. To disable TTL verification, use the **no** form of this command.

ttl-security [disable]

no ttl-security

Syntax Description	disable	(Optional) Prevents the ttl-security command from being inherited from a session group or neighbor group.

Defaults	TTL verification is not enabled for eBGP peers.

Command Modes	Neighbor configuration VRF neighbor configuration Neighbor group configuration Session group configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in VRF neighbor configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **ttl-security** command to enable a lightweight security mechanism to protect eBGP peering sessions from CPU utilization-based and other resource exhaustion-based attacks. These types of attacks are typically brute-force Denial of Service (DoS) attacks that attempt to disable the network by flooding devices in the network with IP packets that contain forged source and destination IP addresses in the packet headers.

This command leverages existing behavior in IP packets. For a given IP packet, the TTL count of the packet always is equal to or less than the TTL count when the packet originated, a behavior that is considered impossible to circumvent. Therefore, a packet received with a TTL count equal to the maximum TTL value of 255 can be sent only by a directly adjacent peer. When the **ttl-security** command is configured for an eBGP neighbor that is directly adjacent, the router accepts only IP packets with a TTL count that is equal to the maximum TTL value.

R3.3 Beta Draft—Cisco Confidential Information

The **ttl-security** command secures the eBGP session in the incoming direction only. In the outbound direction, it causes packets to be sent only with the maximum TTL value so that the BGP neighbor can also verify the TTL value of incoming packets. When this command is enabled, BGP establishes or maintains a session only if the TTL value in the IP packet header is equal to the maximum TTL value. If the value is less than the maximum TTL value, the packet is discarded and an Internet Control Message Protocol (ICMP) message is not generated. This behavior is designed because a response to a forged packet is not necessary.



Note

The **ttl-security** command must be configured on each participating router. Failure to configure this command on both ends of the BGP session results in the session progressing as far as the OpenSent or OpenConfirm state, remaining there until the hold time expires.

The following restrictions apply to the configuration of this command:

- The **ttl-security** command should not be configured for a peer that is already configured with the **neighbor ebgp-multihop** command. The simultaneous configuration of these commands is permitted; however, the **ttl-security** command overrides the **ebgp-multihop** command.
- This command is not supported for internal BGP (iBGP) peers.
- This command is not effective against attacks from a directly adjacent peer that has been compromised.

If you configure this command for a neighbor group or session group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.



Note

If the **ttl-security** command is configured on a neighbor to which the router has an established connection or the router is in the process of establishing a connection, the session must be cleared using the **clear bgp** command.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to enable TTL security for eBGP neighbor 192.168.223.7:

```
RP/0/RP0/CPU0:router(config)# router bgp 65534
RP/0/RP0/CPU0:router(config-bgp)# neighbor 192.168.223.7
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 65507
RP/0/RP0/CPU0:router(config-bgp-nbr)# ttl-security
```

The following example shows how to enable TTL security for multiple eBGP neighbors using a session group:

```
RP/0/RP0/CPU0:router(config)# router bgp 65534
RP/0/RP0/CPU0:router(config-bgp)# session-group ebgp-nbrs
RP/0/RP0/CPU0:router(config-bgp-sngrp)# ttl-security
RP/0/RP0/CPU0:router(config-bgp-sngrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 192.168.223.1
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 65501
RP/0/RP0/CPU0:router(config-bgp-nbr)# use session-group ebgp-nbrs
RP/0/RP0/CPU0:router(config-bgp-nbr)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 192.168.223.2
```

R3.3 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 65502
RP/0/RP0/CPU0:router(config-bgp-nbr)# use session-group ebgp-nbrs
RP/0/RP0/CPU0:router(config-bgp-nbr)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 192.168.223.3
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 65503
RP/0/RP0/CPU0:router(config-bgp-nbr)# use session-group ebgp-nbrs
RP/0/RP0/CPU0:router(config-bgp-nbr)# exit
```

Related Commands

Command	Description
ebgp-multihop	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
session-group	Creates a session group and enters session group configuration mode.
show lpts flows	Displays information about locally terminated packet flows, including the minimum TTL value expected.

R3.3 Beta Draft—Cisco Confidential Information

update-source

To allow internal Border Gateway Protocol (iBGP) sessions to use the IP address from a particular interface as the local address when forming an iBGP session with a neighbor, use the **update-source** command in an appropriate configuration mode. To set the chosen local IP address to the nearest interface to the neighbor, use the **no** form of this command.

update-source *interface-type interface-number*

update-source

Syntax Description	<i>interface-type</i>	Interface type. For more information, use the question mark (?) online help function.
	<i>interface-number</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults	Best local address

Command Modes	Neighbor configuration VRF neighbor configuration Neighbor group configuration Session group configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in VRF neighbor configuration mode.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **update-source** command is commonly used with the loopback interface feature. The loopback interface is defined, and the interface address is used as the endpoint for a BGP session through the **update-source** command. This mechanism allows a BGP session to remain up even if the outbound interface goes down, provided there is another route to the neighbor.

If this command is configured for a neighbor group or session group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to configure this router to use the IP address from the Loopback0 interface when trying to open a session with neighbor 172.20.16.6:

```
RP/0/RP0/CPU0:router(config)# router bgp 110
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.16.6
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 110
RP/0/RP0/CPU0:router(config-bgp-nbr)# update-source Loopback0
```

Related Commands

Command	Description
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
session-group	Creates a session group and enters session group configuration mode.

R3.3 Beta Draft—Cisco Confidential Information

use

To inherit configuration from a neighbor group, session group, or address family group, use the **use** command in an appropriate configuration mode. To discontinue inheritance from a group, use the **no** form of this command.

use { **af-group** *group-name* | **neighbor-group** *group-name* | **session-group** *group-name* }

no use { **af-group** | **neighbor-group** | **session-group** }

Syntax Description

af-group	Specifies an address family group.
<i>group-name</i>	Name of the neighbor group, session group, or address family group from which you want to inherit configuration.
neighbor-group	Specifies a neighbor group.
session-group	Specifies a session group.

Defaults

Inheritance of group characteristics does not occur.

Command Modes

For **use af-group** version:

Address family group configuration
Neighbor address family configuration
Neighbor group address family configuration

For **use neighbor-group** version:

Neighbor group configuration
Neighbor configuration
VRF neighbor configuration

For **use session-group** version:

Neighbor group configuration
Neighbor configuration
VRF neighbor configuration
Session-group configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was supported in VRF neighbor configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information

The **use** command configures inheritance of configuration from an address family group, neighbor group, or session group, which means that any configuration for the group also takes effect for the user of the group.

The configuration inherited depends on the type of group that is specified. The group types are described in the following sections:

Address Family Group

An address family group can specify a configuration for only a single address family. The address family specified when the address family group was defined (through the **af-group** command) must match the address family from which the group is used.

Neighbor Group

A neighbor group (like a neighbor) can have address family-independent configuration and address family-specific configuration. All of these configurations could be inherited.

Session Group

A session group can have only address family-independent configuration and thus only address family-independent configuration is inherited from it.

The following rules govern inheritance to resolve possible conflicting configuration:

1. If a command is configured directly on the neighbor that is using group configuration, the command overrides the value that would be normally inherited from the group.
2. If the neighbor is configured to use a session group (for address family-independent configuration) or an address family group (for address family-specific configuration) and the command is configured for the session group or address family group, that configuration is used.
3. The neighbor group configuration is used:
 - If the command is not configured directly on the neighbor and the neighbor is not using a session group (for address family-independent configuration) or an af-group (for address family-specific configuration).
 - The neighbor is using a neighbor group and the command is configured on the neighbor group.

Typically, all configuration for a neighbor group is inherited, but some characteristics may be masked by a session group or address family group. For an example of this configuration, see the “Examples” section.

If the neighbor is using both a session group and a neighbor group and a specific command is configured for the neighbor group but not for the session group, then the configuration for the neighbor group does not take effect. The session group “hides” all address family-independent configuration on the neighbor group and prevents it from being inherited. Similarly, the use of an address family group hides any address family-specific configuration that may otherwise be inherited from a neighbor group for that address family.

In addition to neighbors using groups, it is possible to build a hierarchy by having groups use other groups. The following hierarchical groups are permitted:

- Session groups may use other session groups.
- Address family groups may use other address family groups.
- Neighbor groups may use other neighbor groups.
- Neighbor groups may use session groups and address family groups.

R3.3 Beta Draft—Cisco Confidential Information



Note

Within the Cisco IOS XR system configuration architecture, do not combine the **remote-as** command and the **no use neighbor-group** command in the same commit, or the **remote-as** command and the **no use session-group** command in the same commit.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to define a session group session1 and configure neighbor 172.168.40.24 to use session1. As a result, the session1 configuration takes effect on the neighbor also.

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# session-group session1
RP/0/RP0/CPU0:router(config-bgp-sngrp)# advertisement-interval 40
RP/0/RP0/CPU0:router(config-bgp-sngrp)# timers 30 90
RP/0/RP0/CPU0:router(config-bgp-sngrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.168.40.24
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 2
RP/0/RP0/CPU0:router(config-bgp-nbr)# use session-group session1
RP/0/RP0/CPU0:router(config-bgp-nbr)# exit
```

The following example is similar to the previous example, but in this case the **timers** command on the session group does not take effect on the neighbor because it is overridden by a **timers** command directly configured for the neighbor.

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# session-group session1
RP/0/RP0/CPU0:router(config-bgp-sngrp)# advertisement-interval 40
RP/0/RP0/CPU0:router(config-bgp-sngrp)# timers 30 90
RP/0/RP0/CPU0:router(config-bgp-sngrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.168.40.24
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 2
RP/0/RP0/CPU0:router(config-bgp-nbr)# use session-group session1
RP/0/RP0/CPU0:router(config-bgp-nbr)# timers 60 180
RP/0/RP0/CPU0:router(config-bgp-nbr)# exit
```

The following example shows an address family group, family1, for IPv4 multicast and a neighbor group, neighbor1, that have IPv4 unicast and IPv4 multicast enabled. In this case, the neighbor inherits IPv4 unicast (and address family-independent) configuration from the neighbor group, but inherits IPv4 multicast configuration from the address family group. In this example, the neighbor group also has a remote autonomous system configured, so there is no need to configure a remote autonomous system for the neighbor because it inherits the remote autonomous system from the neighbor group:

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# af-group family1 address-family ipv4 multicast
RP/0/RP0/CPU0:router(config-bgp-afgrp)# route-policy mcast-in in
RP/0/RP0/CPU0:router(config-bgp-afgrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor-group neighbor1
RP/0/RP0/CPU0:router(config-bgp-nbrgrp)# remote-as 2
RP/0/RP0/CPU0:router(config-bgp-nbrgrp)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbrgrp-af)# route-policy policy1 in
RP/0/RP0/CPU0:router(config-bgp-nbrgrp-af)# route-policy policy1 out
RP/0/RP0/CPU0:router(config-bgp-nbrgrp-af)# exit
RP/0/RP0/CPU0:router(config-bgp-nbrgrp)# address-family ipv4 multicast
RP/0/RP0/CPU0:router(config-bgp-nbrgrp-af)# route-policy policy1 in
RP/0/RP0/CPU0:router(config-bgp-nbrgrp-af)# route-policy policy1 out
```


R3.3 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config-bgp-nbrgrp-af)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.168.40.24
RP/0/RP0/CPU0:router(config-bgp-nbr)# use neighbor-group neighbor1
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 multicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# use af-group family1
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# exit
```

In the previous example, the neighbor uses the policy1 route policy for inbound and outbound IPv4 unicast routes, but uses the mcast-in route policy for inbound IPv4 multicast routes and no policy for outbound IPv4 multicast routes.

The following example shows a neighbor inheriting configuration from a session group that likewise inherits configuration from another session group. The configuration from both session groups take effect on the neighbor:

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# session-group session1
RP/0/RP0/CPU0:router(config-bgp-sngrp)# advertisement-interval 40
RP/0/RP0/CPU0:router(config-bgp-sngrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# session-group session2
RP/0/RP0/CPU0:router(config-bgp-sngrp)# use session-group session1
RP/0/RP0/CPU0:router(config-bgp-sngrp)# update-source Loopback0
RP/0/RP0/CPU0:router(config-bgp-sngrp)# exit
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.168.40.24
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# use session-group session2
RP/0/RP0/CPU0:router(config-bgp-nbr)# exit
```

Related Commands

Command	Description
af-group	Creates an address family group for BGP neighbors and enters address family group configuration mode.
session-group	Creates a session group and enters session group configuration mode.
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
remote-as (BGP)	Creates a BGP neighbor and begins the exchange of routing information.
show bgp af-group	Displays information about BGP configuration for address family groups.
show bgp neighbor-group	Displays information about the BGP configuration for neighbor groups.
show bgp neighbors	Displays information about BGP neighbors.
show bgp session-group	Displays information about the BGP configuration for session groups.

R3.3 Beta Draft—Cisco Confidential Information

vrf

To configure a VPN routing and forwarding (VRF) instance and enter VRF configuration mode, use the **vrf** command in router configuration mode. To remove the VRF instance from the configuration file and restore the system to its default condition, use the **no** form of this command.

vrf *vrf-name*

no vrf *vrf-name*

Syntax Description

<i>vrf-name</i>	Name of the VRF instance. The following names cannot be used: all, default, and global.

Defaults

No default behavior or values

Command Modes

Router configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **vrf** command to configure a VRF instance. A VRF instance is a collection of VPN routing and forwarding tables maintained at the provider edge (PE) router.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to configure a VRF instance and enter VRF configuration mode:

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# vrf vrf-1
RP/0/RP0/CPU0:router(config-bgp-vrf)#
```

R3.3 Beta Draft—Cisco Confidential Information

weight

To assign a weight to routes received from a neighbor, use the **weight** command in an appropriate configuration mode. To remove the **weight** command from the configuration file and restore the system to its default condition in which the software assigns the default weight to routes, use the **no** form of this command.

weight *weight-value*

no weight

Syntax Description	<i>weight-value</i>	Weight to assign. Range is 0 to 65535.

Defaults	Routes learned through another Border Gateway Protocol (BGP) peer have a default weight of 0 and routes sourced by the local router have a default weight of 32768.

Command Modes	IPv4 address family group configuration IPv6 address family group configuration VPNv4 address family group configuration IPv4 neighbor address family configuration VPNv4 neighbor address family configuration VRF IPv4 neighbor address family configuration IPv4 neighbor group address family configuration IPv6 neighbor group address family configuration VPNv4 neighbor group address family configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was supported in the following configuration modes: - VPNv4 address family group - VPNv4 neighbor address family - VRF IPv4 neighbor address family - VPNv4 neighbor group address family

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

The weight assigned to individual routes may be modified by using an inbound routing policy.

R3.3 Beta Draft—Cisco Confidential Information



Note

For weight changes to take effect, you may need to use the **clear bgp** command.

If this command configures a neighbor group or neighbor address family group, all neighbors using the group inherit the configuration. Values of commands configured specifically for a neighbor override inherited values.

Task ID

Task ID	Operations
bgp	read, write

Examples

The following example shows how to assign a weight of 50 to all IP Version 4 (IPv4) unicast routes learned through 172.20.16.6:

```
RP/0/RP0/CPU0:router(config)# router bgp 1
RP/0/RP0/CPU0:router(config-bgp)# neighbor 172.20.16.6
RP/0/RP0/CPU0:router(config-bgp-nbr)# remote-as 1
RP/0/RP0/CPU0:router(config-bgp-nbr)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# weight 50
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# exit
```

Related Commands

Command	Description
af-group	Creates an address family group for BGP neighbors and enters address family group configuration mode.
clear bgp	Resets a group of BGP neighbors.
neighbor-group	Creates a neighbor group and enters neighbor group configuration mode.
session-group	Creates a session group and enters session group configuration mode.

EIGRP Commands on Cisco IOS XR Software

Beta Draft Cisco Confidential Information

This chapter describes the commands used to configure and monitor the Enhanced Interior Gateway Routing Protocol (EIGRP).

For detailed information about EIGRP concepts, configuration tasks, and examples, see the *Implementing EIGRP on Cisco IOS XR Software* configuration guide.

R3.3 Beta Draft—Cisco Confidential Information

address-family ipv4 (EIGRP)

To enter IPv4 address family configuration mode to configure an Enhanced Interior Gateway Routing Protocol (EIGRP), use the **address-family ipv4** command in the appropriate mode. To remove the address family from the EIGRP configuration, use the **no** form of this command.

address-family ipv4

no address-family ipv4

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Router configuration
VRF configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **address-family ipv4** command to configure IPv4 address family sessions under EIGRP. To leave address family configuration mode without removing the address family configuration, use the **exit-address-family** command.

In addition, EIGRP Virtual Private Networks (VPNs) can be configured under IPv4 address family configuration mode after first entering VRF configuration mode. A VPN routing and forwarding instance (VRF) and route distinguisher must be defined before the VRF address family session can be created. From within VRF, all EIGRP commands, are configurable except the **autonomous-system** and **maximum-prefix** commands.

A single EIGRP routing process can support multiple VRFs. The number of VRFs that can be configured is limited by only available system resources on the router, which is determined by the number of VRFs, running processes, and available memory. However, only a single VRF can be supported by each VPN, and redistribution between different VRFs is not supported.

MPLS VPN support between PE and CE routers is configured only on PE routers that provide VPN services over the service provider backbone. The customer site does not require any changes to equipment or configurations to support the EIGRP VPN. A metric must be configured for routes to be advertised to the CE router. The metric can be configured using the **redistribute protocol** command or configured with the **default-metric (EIGRP)** command.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	eigrp	read, write

Examples

The following example shows how to configure a IPv4 VRF address family session after defining the VRF named vrf1:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp)# vrf vrf1
RP/0/RP0/CPU0:router(config-eigrp-vrf)# address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-vrf-af)# autonomous-system 101
RP/0/RP0/CPU0:router(config-eigrp-vrf-af)# default-metric 1000 100 255 1 1500
RP/0/RP0/CPU0:router(config-eigrp-vrf-af)# exit-address-family
```

Related Commands

Command	Description
default-metric (EIGRP)	Sets metrics for an EIGRP.
redistribute (EIGRP)	Redistributes routes from one routing domain into EIGRP.

R3.3 Beta Draft—Cisco Confidential Information

auto-summary (EIGRP)

To allow automatic summarization of subnet routes into network-level routes for an Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the **auto-summary** command in the appropriate configuration mode. To disable this function 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.

Defaults The behavior of this command is disabled by default (the software sends subprefix routing information across classful network boundaries).

Command Modes Address family configuration
IPv4 VRF address family configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Route summarization reduces the amount of routing information in the routing tables.

By default, Border Gateway Protocol (BGP) does not accept subnets redistributed from an Interior Gateway Protocol (IGP). Use the **auto-summary** command to allow the software to create summary subprefixes to the classful network boundary when crossing classful network boundaries.

Enhanced Interior Gateway Routing Protocol (EIGRP) summary routes are given an administrative distance value of 5. You cannot configure this value.

If you are using Routing Information Protocol (RIP) Version 2, you can turn off automatic summarization by specifying the **no auto-summary** command. Disable automatic summarization if you must perform routing between disconnected subnets. When automatic summarization is off, subnets are advertised.

Task ID	Task ID	Operations
	eigrp	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to enable automatic summarization for EIGRP 1:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1  
RP/0/RP0/CPU0:router(config-eigrp)# vrf vpn-1  
RP/0/RP0/CPU0:router(config-eigrp-vrf)# address-family ipv4  
RP/0/RP0/CPU0:router(config-eigrp-vrf-af)# auto-summary
```

Related Commands

Command	Description
summary-address (EIGRP)	Configures a summary aggregate address for a specified interface.

R3.3 Beta Draft—Cisco Confidential Information

autonomous-system

To configure an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process to run within a VPN routing and forwarding instance (VRF), use the **autonomous-system** command in IPv4 VRF address family configuration mode.

autonomous-system *as-number*

Syntax Description	<i>as-number</i>	Autonomous system number of the EIGRP routing process.

Defaults	No default behavior or values

Command Modes	IPv4 VRF address family configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the autonomous-system command only after a VRF name is specified when entering address family configuration mode.

Task ID	Task ID	Operations
	eigrp	read, write

Examples	The following example shows how to configure autonomous system 101 under VRF VPN-1:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp)# vrf vpn-1
RP/0/RP0/CPU0:router(config-eigrp-vrf)# address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-vrf-af)# autonomous-system 101
```

Related Commands	Command	Description
	vrf (EIGRP)	Defines a VRF instance and to enters VRF configuration mode.

R3.3 Beta Draft—Cisco Confidential Information

bandwidth-percent (EIGRP)

To configure the percentage of bandwidth that may be used by EIGRP on an interface, use the **bandwidth-percent** command in interface configuration mode. To restore the default value, use the **no** form of this command.

bandwidth-percent *as-number percent*

no bandwidth-percent

Syntax Description	<i>as-number</i>	Autonomous system number.
	<i>percent</i>	Percentage of bandwidth that EIGRP may use.

Defaults	<i>percent</i> : 50

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	EIGRP uses up to 50 percent of the bandwidth of a link, as defined by the bandwidth interface configuration command. This command may be used if some other fraction of the bandwidth is desired. Values greater than 100 percent may be configured. The configuration option may be useful if the bandwidth is set artificially low for other reasons.

Task ID	Task ID	Operations
	eigrp	read, write

Examples	The following example shows how to configure EIGRP to use up to 75 percent (42 kbps) of an interface in autonomous system 209:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp)# address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-af)# router-id 10.1.1.1
RP/0/RP0/CPU0:router(config-eigrp-af)# interface POS 0/1/0/0
RP/0/RP0/CPU0:router(config-eigrp-af-if)# bandwidth-percent 209 75
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	bandwidth (interface)	Sets a bandwidth value for an interface.

R3.3 Beta Draft—Cisco Confidential Information

clear eigrp events

To delete Enhanced Interior Gateway Routing Protocol (EIGRP) and VRF entries from the appropriate table, use the **clear eigrp events** command in EXEC mode.

clear eigrp [*as-number* | **vrf** {*vrf* | **all**}] **events**

Syntax Description

<i>as-number</i>	(Optional) Autonomous system number. Range is from 1 to 65535.
vrf { <i>vrf</i> all }	(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances.

Defaults

When no autonomous system number or VRF instance is specified, all EIGRP event entries are cleared from the table.

Command Modes

EXEC

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
eigrp	read, write

Examples

The following example shows how to clear EIGRP events for autonomous system 10:

```
RP/0/RP0/CPU0:router# clear eigrp 10 events
```

Related Commands

Command	Description
show eigrp interfaces	Displays information about interfaces configured for EIGRP.

R3.3 Beta Draft—Cisco Confidential Information

clear eigrp logging

To delete Enhanced Interior Gateway Routing Protocol (EIGRP) and VRF logging entries from the appropriate table, use the **clear eigrp logging** command in EXEC mode.

clear eigrp [*as-number* | **vrf** {*vrf* | **all**}] **logging**

Syntax Description

<i>as-number</i>	(Optional) Autonomous system number. Range is from 1 to 65535.
vrf { <i>vrf</i> all }	(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances.

Defaults

When no autonomous system number or VRF instance is specified, all EIGRP logging entries are cleared from the table.

Command Modes

EXEC

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
eigrp	read, write

Examples

The following example shows how to clear EIGRP logging entries for autonomous system 10:

```
RP/0/RP0/CPU0:router# clear eigrp 10 logging
```

Related Commands

Command	Description
show eigrp interfaces	Displays information about interfaces configured for EIGRP.

R3.3 Beta Draft—Cisco Confidential Information

clear eigrp neighbors

To delete Enhanced Interior Gateway Routing Protocol (EIGRP) and Virtual Private Network (VPN) neighbor entries from the appropriate table, use the **clear eigrp neighbors** command in EXEC mode.

clear eigrp [*as-number* | **vrf** {*vrf* | **all**}] **neighbors** [*ip-address* | *interface-type interface-instance*]

Syntax Description	
<i>as-number</i>	(Optional) Autonomous system number. Range is from 1 to 65535.
vrf { <i>vrf</i> all }	(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances.
<i>ip-address</i>	(Optional) Address of the neighbor.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance. Specifying these arguments removes the specified interface type from the neighbor table that all entries learned via this interface. - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults When no autonomous system number or VRF instance is specified, all EIGRP neighbor entries are cleared from the table.

Command Modes EXEC

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

R3.3 Beta Draft – Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
eigrp	read, write

Examples

The following example shows how to clear all EIGRP VRF entries for neighbor Gigabit Ethernet interface 0/5/0/0:

```
RP/0/RP0/CPU0:router# clear eigrp vrf all neighbors GigabitEthernet 0/5/0/0
```

Related Commands

Command	Description
show eigrp interfaces	Displays information about interfaces configured for EIGRP.

R3.3 Beta Draft—Cisco Confidential Information

clear eigrp topology

To delete Enhanced Interior Gateway Routing Protocol (EIGRP) and VRF topology entries from the appropriate table, use the **clear eigrp topology** command in EXEC mode.

clear eigrp [*as-number* | **vrf** {*vrf* | **all**}] **topology** [*prefix mask*] [*prefix/length*]

Syntax Description	<i>as-number</i>	(Optional) Autonomous system number. Range is from 1 to 65535.
	vrf { <i>vrf</i> all }	(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances.
	<i>prefix</i>	(Optional) IP prefix, which limits output to a specific route. If the <i>prefix</i> argument is specified, either the <i>length</i> or <i>mask</i> argument is required.
	<i>mask</i>	(Optional) IP address mask.
	<i>length</i>	(Optional) Prefix length, which can be indicated as a slash (/) and number. For example, /8 indicates that the first eight bits in the IP prefix are network bits. If <i>length</i> is used, the slash is required.

Defaults	When no autonomous system number or VRF instance is specified, all EIGRP topology entries are cleared from the table.

Command Modes	EXEC

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	eigrp	read, write

Examples	The following example shows how to clear EIGRP topology entries for a specific route:

```
RP/0/RP0/CPU0:router# clear eigrp topology 10.1.0.0/8
```

 clear eigrp topology

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	show eigrp interfaces	Displays information about interfaces configured for EIGRP.

R3.3 Beta Draft—Cisco Confidential Information

default-information

To control the candidate default routing information for an Enhanced Interior Gateway Routing Protocol (EIGRP), use the **default-information** command in the appropriate configuration mode. To suppress EIGRP candidate information in incoming or outgoing updates, use the **no** form of this command.

default-information accept {in | out}[route-policy *name*]

no default-information accept {in | out}[route-policy *name*]

Syntax Description

accept	Specifies EIGRP to accept default routing information.
in	Specifies EIGRP to accept inbound default routing information.
out	Specifies EIGRP to accept outbound default routing information.
route-policy <i>name</i>	(Optional) Specifies a route policy.

Defaults

Typically, outgoing routes are always accepted and default information is passed between EIGRP processes when redistribution occurs.

Command Modes

Address family configuration
IPv4 VRF address family configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The default network of 0.0.0.0 used by Routing Information Protocol (RIP) cannot be redistributed by IGRP, but can be redistributed by EIGRP.

Task ID

Task ID	Operations
eigrp	read, write

Examples

The following example shows how to configure inbound default routes specified with route policy acme to be accepted by an EIGRP peer in autonomous system 1:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp)# vrf vrf1
RP/0/RP0/CPU0:router(config-eigrp-vrf)# address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-vrf-af)# default-information accept in route-policy acme
```

R3.3 Beta Draft—Cisco Confidential Information**default-metric (EIGRP)**

To set metrics for an Enhanced Interior Gateway Routing Protocol (EIGRP), use the **default-metric** command in the appropriate configuration mode. To remove the metric value and restore the default state, use the **no** form of this command.

default-metric *bandwidth delay reliability loading mtu*

no default-metric

Syntax Description	
<i>bandwidth</i>	Minimum bandwidth of the route in kilobits per second. Range is 1 to 4294967295.
<i>delay</i>	Route delay in tens of microseconds. Delay is 1 or any positive number that is a multiple of 39.1 nanoseconds. Range is 1 to 4294967295.
<i>reliability</i>	Likelihood of successful packet transmission expressed as a number between 0 and 255. The value 255 means 100-percent reliability; 0 means no reliability.
<i>loading</i>	Effective bandwidth of the route expressed as a number from 1 to 255 (255 is 100-percent loading).
<i>mtu</i>	Minimum maximum transmission unit (MTU) size of the route in bytes. Range is from 1 to 65535.

Defaults Only connected routes can be redistributed without a default metric. The metric of redistributed connected routes is set to 0.

Command Modes Address family configuration
IPv4 VRF address family configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **default-metric** command to redistribute a protocol into EIGRP, unless you use the **redistribute protocol** command. Automatic metric translations occur between EIGRP. You do not need default metrics to redistributed EIGRP into itself.

**Note**

The **default-metric** command does not affect EIGRP-to-EIGRP distribution. To configure EIGRP-to-EIGRP distribution, use route policies.

R3.3 Beta Draft—Cisco Confidential Information

Metric defaults have been carefully set to work for a wide variety of networks. Take great care when changing these values.

Keeping the same metrics is supported only when redistributing from EIGRP or static routes.

Task ID	Task ID	Operations
	eigrp	read, write

Examples

The following example shows how to take redistributed Routing Information Protocol (RIP) metrics and translate them into EIGRP metrics with values as follows: bandwidth = 1000, delay = 100, reliability = 250, loading = 100, and MTU = 1500.

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp)# vrf vrf1
RP/0/RP0/CPU0:router(config-eigrp-vrf)# address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-vrf-af)# redistribute rip
RP/0/RP0/CPU0:router(config-eigrp-vrf-af)# default-metric 1000 100 250 100 1500
```

Related Commands	Command	Description
	redistribute	Redistributes routes from one routing domain into another routing domain.

R3.3 Beta Draft—Cisco Confidential Information

distance (EIGRP)

To allow the use of two administrative distances—internal and external—that could be a better route to a node, use the **distance** command in the appropriate configuration mode. To reset these values to their defaults, use the **no** form of this command.

distance *internal-distance external-distance*

no distance

Syntax Description

<i>internal-distance</i>	Administrative distance for EIGRP internal routes. Internal routes are those that are learned from another entity within the same autonomous system. The distance can be a value from 1 to 255.
<i>external-distance</i>	Administrative distance for EIGRP external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. The distance can be a value from 1 to 255.

Defaults

internal-distance: 90
external-distance: 170

Command Modes

Address family configuration
 IPv4 VRF address family configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

An administrative distance is 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 an integer from 0 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 the **distance** command if another protocol is known to provide a better route to a node than was actually learned through the external Enhanced Interior Gateway Routing Protocol (EIGRP), or if some internal routes should be preferred by EIGRP.

R3.3 Beta Draft—Cisco Confidential Information

Table 36 lists the default administrative distances.

Table 36 Default Administrative Distances

Route Source	Default Distance
Connected interface	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
Open Shortest Path First (OSPF)	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
EIGRP external route	170
Internal Border Gateway Protocol (BGP)	200
Unknown	255

To display the default administrative distance for a specified routing process, use the **show protocols EXEC** command.

Task ID	Task ID	Operations
	eigrp	read, write

Examples

The following example shows how to set the administrative distance of all EIGRP 1 internal routes (within vrf vpn-1) to 80 and all EIGRP external routes to 130:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp)# vrf vrf1
RP/0/RP0/CPU0:router(config-eigrp-vrf)# address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-vrf-af)# distance 80 130
```

Related Commands	Command	Description
	show protocols	Displays routing protocol instance information that is running on the router.

R3.3 Beta Draft—Cisco Confidential Information

hello-interval (EIGRP)

To configure the hello interval for the Enhanced Interior Gateway Routing Protocol (EIGRP) routing process, use the **hello-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

hello-interval *seconds*

no hello-interval *seconds*

Syntax Description	<i>seconds</i>	Hello interval (in seconds). The range is from 1 to 65535.

Defaults	For low-speed, nonbroadcast multiaccess (NBMA) networks: 60 seconds For all other networks: 5 seconds

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	eigrp	read, write

Examples	The following example shows how to set the hello interval to 0 to 10 seconds for the interface: <pre>RP/0/RP0/CPU0:router(config)# router eigrp 1 RP/0/RP0/CPU0:router(config-eigrp)# address-family ipv4 RP/0/RP0/CPU0:router(config-eigrp)# router-id 10.1.1.1 RP/0/RP0/CPU0:router(config-eigrp-af)# interface POS 0/1/0/0 RP/0/RP0/CPU0:router(config-eigrp-af-if)# hello-interval 109 10</pre>

R3.3 Beta Draft—Cisco Confidential Information

hold-time (EIGRP)

To configure the hold time for a particular Enhanced Interior Gateway Routing Protocol (EIGRP) routing process, use the **hold-time** command in interface configuration mode. To restore the default value, use the **no** form of this command.

hold-time *seconds*

no hold-time

Syntax Description	<i>seconds</i>	Hold time (in seconds). The range is from 1 to 65535.

Defaults

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

On very congested and large networks, the default hold time might not be sufficient time for all routers to receive hello packets from their neighbors. In this case, you may want to increase the hold time.

We recommend that the hold time be at least three times the hello interval. If a router does not receive a hello packet within the specified hold time, routes through this router are considered unavailable.

Increasing the hold time delays route convergence across the network.

The default of 180 seconds hold time and 60 seconds hello interval apply only to low-speed, NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command.

Task ID	Task ID	Operations
	eigrp	read, write

Examples	The following example shows how to set the hold time to 0 to 40 seconds for the interface:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp)# address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp)# router-id 10.1.1.1
```

R3.3 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config-eigrp-af)# interface POS 0/1/0/0  
RP/0/RP0/CPU0:router(config-eigrp-af-if)# hold-time 109 40
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
hello-interval (EIGRP)	Configures the hello interval for the EIGRP routing process designated by an autonomous system number.

R3.3 Beta Draft—Cisco Confidential Information

interface (EIGRP)

To define the interfaces on which the Enhanced Interior Gateway Routing Protocol (EIGRP) routing protocol runs, use the **interface** command in the appropriate configuration mode. To disable EIGRP routing for interfaces, use the **no** form of this command.

interface *type instance*

no interface *type instance*

Syntax Description	
<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults	When you do not specify this command in configuration mode, EIGRP routing for interfaces is not enabled.

Command Modes	Address family configuration IPv4 VRF address family configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the interface command to associate a specific interface with an EIGRP process. The interface remains associated with the process even when the IPv4 address of the interface changes.

R3.3 Beta Draft—Cisco Confidential Information

This command places the router in interface configuration mode, from which you can configure interface-specific settings. Commands configured under this mode (such as the **hello-interval** command) are automatically bound to that interface.

Task ID	Task ID	Operations
	eigrp	read, write

Examples

The following example shows how to enter interface configuration mode for EIGRP process 1 and set the hello interval to 10 seconds for the Packet-over-SONET/SDH (POS) interface 0/1/0/0:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp)# address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp)# router-id 10.1.1.1
RP/0/RP0/CPU0:router(config-eigrp-af)# interface POS 0/1/0/0
RP/0/RP0/CPU0:router(config-eigrp-af-if)# hello-interval 109 10
```

Related Commands	Command	Description
	hello-interval (EIGRP)	Configures the hello interval for the EIGRP routing process designated by an autonomous system number.

R3.3 Beta Draft—Cisco Confidential Information

log-neighbor-changes

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, use the **log-neighbor-changes** command in the appropriate configuration mode. To disable the logging of changes in EIGRP neighbor adjacencies, use the **no** form of this command.

log-neighbor-changes

no log-neighbor-changes

Syntax Description This command has no arguments or keywords.

Defaults Adjacency changes are logged.

Command Modes Address family configuration
IPv4 VRF address family configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **log-neighbor-changes** command to log neighbor adjacency changes, monitor the stability of the routing system, and help detect problems. Logging is enabled by default. To disable the logging of neighbor adjacency changes, use the **no** form of this command.

Task ID	Task ID	Operations
	eigrp	read, write

Examples The following example shows how to enable logging of neighbor changes for EIGRP 1:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp)# address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-af)# log-neighbor-changes
```

R3.3 Beta Draft—Cisco Confidential Information

log-neighbor-warnings

To enable the logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor warning messages, use the **log-neighbor-warnings** command in the appropriate configuration mode. To disable the logging of EIGRP neighbor warning messages, use the **no** form of this command.

log-neighbor-warnings

no log-neighbor-warnings

Syntax Description This command has no arguments or keywords.

Defaults Neighbor warning messages are logged.

Command Modes Address family configuration
IPv4 VRF address family configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **log-neighbor-warnings** command to disable and enable neighbor warning messages. When neighbor warning messages occur, they are logged by default.

Task ID	Task ID	Operations
	eigrp	read, write

Examples The following example shows how to configure log neighbor warning messages for EIGRP process 20:

```
RP/0/RP0/CPU0:router(config)# router eigrp 20
RP/0/RP0/CPU0:router(config-eigrp) vrf vrf1
RP/0/RP0/CPU0:router(config-eigrp-vrf)# address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-vrf-af)# log-neighbor-warnings
```

R3.3 Beta Draft—Cisco Confidential Information

maximum-paths (EIGRP)

To control the maximum number of parallel routes that the Enhanced Interior Gateway Routing Protocol (EIGRP) can support, use the **maximum-paths** command in the appropriate configuration mode. To remove the **maximum-paths** command from the configuration file and restore the system to its default condition with respect to the routing protocol, use the **no** form of this command.

maximum-paths *maximum*

no maximum-paths

Syntax Description	<i>maximum</i>	Maximum number of parallel routes that EIGRP can install in a routing table.

Defaults

Command Modes	Address family configuration IPv4 VRF address family configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the maximum-paths command to allow the EIGRP protocol to install multiple paths into the routing table for each prefix. Multiple paths are installed for external peers that are from the same autonomous system and are equal cost (according to the EIGRP best path algorithm). Similarly, multiple paths are installed for internal peers that are equal cost (based on the EIGRP best path algorithm).

Task ID	Task ID	Operations
	eigrp	read, write

Examples	The following example shows how to allow a maximum of 10 paths to a destination:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp) vrf vrf1
RP/0/RP0/CPU0:router(config-eigrp-vrf)# address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-vrf-af)# maximum-paths 10
```

R3.3 Beta Draft—Cisco Confidential Information**maximum-prefix (EIGRP)**

To limit the number of prefixes that are accepted under an address family by Enhanced Interior Gateway Routing Protocol (EIGRP), use the **maximum-prefix** command in address family configuration mode. To disable this function, use the **no** form of this command.

maximum-prefix *maximum* [*threshold*] [**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] [**warning-only**]

no maximum-prefix *maximum* [*threshold*] [**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] [**warning-only**]

Syntax Description		
<i>maximum</i>	Maximum number of prefixes allowed under an address family. Range is from 1 to 4294967295.	
	Note	The number of prefixes that can be configured is limited only by the available system resources on the router.
<i>threshold</i>	(Optional) Syslog warning messages are specified as a percentage of the maximum prefix limit that was exceeded. The prefix percentage number range is from 1 to 100. The default is 75 percent.	
dampened	(Optional) A decay penalty is applied to the restart time period each time the maximum prefix limit is exceeded. The half-life for the decay penalty is 150% of the default or user-defined restart time value in minutes. This keyword is disabled by default.	
reset-time <i>minutes</i>	(Optional) The restart count is reset to 0 after the default or user-defined reset time period has expired. The range of values that can be applied with the <i>minutes</i> argument is from 1 to 65535 minutes. The default reset-time period is 15 minutes.	
restart <i>minutes</i>	(Optional) A time period when router adjacencies are not formed or when redistributed routes are not accepted from the RIB after the maximum prefix limit has been exceeded. The value for the <i>minutes</i> argument is from 1 to 65535 minutes. The default restart time period is 5 minutes.	
restart-count <i>number</i>	(Optional) Number of times a peering session is automatically reestablished after the peering session is torn down or after the redistribute route is cleared and relearned when the maximum prefix exceeds limits. The default restart count limit is 3.	
		
	Caution	Once the restart count threshold is crossed, you need to use the clear route or clear eigrp neighbors command to reestablish normal peering and/or redistribution.
warning-only	(Optional) Configures the router to generate syslog messages only when the maximum prefix limit is reached, instead of terminating the peering session.	

R3.3 Beta Draft—Cisco Confidential Information

Defaults

threshold: 75 percent
 reset-time: 15 minutes
 restart: 5 minutes
 restart-count: 3

Command Modes

IPv4 VRF address family configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **maximum-prefix** command to limit the number of prefixes that are accepted from all sources. When the maximum prefix limit is exceeded, sessions with remote peers are torn down, all routes learned from remote peers and through redistribution are removed from the topology and routing tables, and redistribution and peering are suspended for the default or user-defined time period.

Task ID

Task ID	Operations
eigrp	read, write

Examples

The following example shows how to configure the maximum prefix limit for an EIGRP process, which includes routes learned through redistribution and routes learned through EIGRP peering sessions. The maximum limit is set to 50,000 prefixes. When the number of prefixes learned through redistribution reaches 37,500 (75 percent of 50,000), warning messages are displayed in the console. When the maximum prefix limit is exceeded, all peering sessions are reset, the topology and routing tables are cleared and redistributed routes and all peering sessions are placed in a penalty state.

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp)# vrf vrf1
RP/0/RP0/CPU0:router(config-eigrp-vrf)# address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-vrf-af)# maximum-prefix 50000
```

Related Commands

Command	Description
clear eigrp neighbors	Deletes EIGRP VPN neighbor entries from the table.
clear route	Deletes routes from the IP routing table.

R3.3 Beta Draft—Cisco Confidential Information

metric holddown

To prevent the use of new Enhanced Interior Gateway Routing Protocol (EIGRP) routing information for a certain period of time, use the **metric holddown** command in the appropriate configuration mode. To disable this command, use the **no** form of this command.

metric holddown

no metric holddown

Syntax Description This command has no arguments or keywords.

Command Modes Address family configuration
IPv4 VRF address family configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **metric holddown** command if other routers or access servers within the EIGRP autonomous system are not configured with the **no metric holddown** command. If all routers are not configured the same way, you increase the possibility of routing loops.

The holddown state keeps new routing information from being used for a certain period of time. This function can prevent routing loops caused by slow convergence. It is sometimes advantageous to disable the holddown state to increase the ability of the network to quickly respond to topology changes; this command provides this function.

Task ID	Task ID	Operations
	eigrp	read, write

Examples The following example shows how to disable metric holddown:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp) address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-af)# no metric holddown
```

R3.3 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	metric maximum-hops	Causes the IP routing software to advertise as unreachable those routes with a hop count higher than is specified by the command (IGRP only).
	metric weights	Allows the tuning of the EIGRP metric calculations.

R3.3 Beta Draft—Cisco Confidential Information

metric maximum-hops

To advertise as unreachable those Enhanced Interior Gateway Routing Protocol (EIGRP) routes with a hop count higher than is specified by the command, use the **metric maximum-hops** command in the appropriate configuration mode. To reset the value to the default, use the **no** form of this command.

metric maximum-hops {hops-number}

no metric maximum-hops

Syntax Description	<i>hops-number</i> Maximum hop count. The range is from 0 to 255 hops.	
Defaults	<i>hops-number</i> : 100	
Command Modes	Address family configuration IPv4 VRF address family configuration	
Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the metric maximum-hops command to provide a safety mechanism that breaks any potential <i>count-to-infinity</i> problems. This command causes the EIGRP routing protocol to advertise as unreachable routes with a hop count greater than the value assigned to the <i>hops-number</i> argument.	
Task ID	Task ID	Operations
	eigrp	read, write
Examples	The following example shows how to configure a hop count to 200 for a router that has a complex WAN generating a large hop count under normal (nonlooping) operations.	

R3.3 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	metric holddown	Keeps new EIGRP routing information from being used for a certain period of time.
	metric weights	Allows the tuning of the EIGRP metric calculations.

R3.3 Beta Draft—Cisco Confidential Information

metric weights

To allow the tuning of the Enhanced Interior Gateway Routing Protocol (EIGRP) metric calculations, use the **metric weights** command in the appropriate configuration mode. To reset the values to their defaults, use the **no** form of this command.

metric weights *tos k1 k2 k3 k4 k5*

no metric weights

Syntax Description	<i>tos</i>	Type of service (ToS) which must always be zero.
	<i>k1 k2 k3 k4 k5</i>	Constants that convert an EIGRP metric vector into a scalar quantity.

Defaults	<i>tos</i> : 0
	<i>k1</i> : 1
	<i>k2</i> : 0
	<i>k3</i> : 1
	<i>k4</i> : 0
	<i>k5</i> : 0

Command Modes	Address family configuration
	IPv4 VRF address family configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **metric weights** command to alter the default behavior of EIGRP routing and metric computation and allow the tuning of the EIGRP metric calculation for a particular ToS.

If *k5* equals 0, the composite EIGRP metric is computed according to the following formula:

$$\text{metric} = [k1 * \text{bandwidth} + (k2 * \text{bandwidth}) / (256 - \text{load}) + k3 * \text{delay}]$$

If *k5* does not equal zero, an additional operation is performed:

$$\text{metric} = \text{metric} * [k5 / (\text{reliability} + k4)]$$

Bandwidth is inverse minimum bandwidth of the path in BPS scaled by a factor of $2.56 * 10^{12}$. The range is from a 1200-bps line to 10 terabits per second.

R3.3 Beta Draft—Cisco Confidential Information

Delay is in units of 10 microseconds. The range of delay is from 10 microseconds to 168 seconds. A delay of all 1s indicates that the network is unreachable.

The delay parameter is stored in a 32-bit field, in increments of 39.1 nanoseconds. The range of delay is from 1 (39.1 nanoseconds) to hexadecimal FFFFFFFF (decimal 4,294,967,040 nanoseconds). A delay of all 1s (that is, a delay of hexadecimal FFFFFFFF) indicates that the network is unreachable.

Table 37 lists the default values used for several common media.

Table 37 Bandwidth Values by Media Type

Media Type	Delay	Bandwidth
Satellite	5120 (2 seconds)	5120 (500 megabits)
Ethernet	25600 (1 milliseconds [ms])	256000 (10 megabits)
1.544 Mbps	512000 (20,000 ms)	1,657,856 bits
64 kbps	512000 (20,000 ms)	40,000,000 bits
56 kbps	512000 (20,000 ms)	45,714,176 bits
10 kbps	512000 (20,000 ms)	256,000,000 bits
1 kbps	512000 (20,000 ms)	2,560,000,000 bits

Reliability is given as a fraction of 255. That is, 255 is a reliability of 100 percent or a perfectly stable link. Load is given as a fraction of 255. A load of 255 indicates a completely saturated link.

Task ID

Task ID	Operations
eigrp	read, write

Examples

The following example shows how to set the metric weights to change the default values:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp) address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-af)# metric weights 0 2 0 2 0 0
```

Related Commands

Command	Description
metric holddown	Keeps new EIGRP routing information from being used for a certain period of time.
metric maximum-hops	Advertises as unreachable those EIGRP VPN routes with a hop count higher than is specified by the command.

R3.3 Beta Draft—Cisco Confidential Information

neighbor maximum-prefix

To limit the number of prefixes that are accepted from a single Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor or all EIGRP VPN neighbors, use the **neighbor maximum-prefix** command in IPv4 VRF address family configuration mode. To disable this function, use the **no** form of this command.

Single-Neighbor Configuration CLI

neighbor *ip-address* **maximum-prefix** *maximum* [*threshold*] [**warning-only**]

no neighbor *ip-address* **maximum-prefix**

All-Neighbor Configuration CLI

neighbor maximum-prefix *maximum* [*threshold*] [**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] [**warning-only**]

no neighbor maximum-prefix

Syntax Description

<i>ip-address</i>	(Optional) IP address of a single peer.
<i>maximum</i>	Maximum number of prefixes accepted. The range is from 1 to 4294967295.
	Note The number of prefixes that can be configured is limited only by the available system resources on the router.
<i>threshold</i>	(Optional) Syslog warning messages are specified as a percentage of the maximum prefix limit that was exceeded. The prefix percentage number range is from 1 to 100. The default is 75 percent.
dampened	(Optional) Configures a decay penalty to be applied to the restart time period each time the maximum prefix limit is exceeded. The half-life for the decay penalty is 150 percent of the default or user-defined restart time value in minutes. This keyword is disabled by default.
reset-time <i>minutes</i>	(Optional) Configures the router to reset the restart count to 0 after the default or configured reset time period has expired. The range is from 1 to 65535 minutes.
restart <i>minutes</i>	(Optional) Configures a time period in which the router does not form adjacencies or accept redistributed routes from the RIB after the maximum prefix limit has been exceeded. The range is from 1 to 65535 minutes.

R3.3 Beta Draft—Cisco Confidential Information

restart-count <i>number</i>	(Optional) Configures the number of times a peering session can be automatically reestablished after the peering session has been torn down or a redistribute route has been cleared and relearned because the maximum prefix limit has been exceeded.



Caution

After the restart count threshold is crossed, you need to use the **clear route** or **clear eigrp neighbors** command to reestablish normal peering, redistribution, or both.

warning-only	(Optional) Configures the router to generate syslog messages only when the maximum prefix limit is reached, instead of terminating the peering session.

Defaults

threshold: 75 percent
dampened: disabled
warning-only: disabled
reset-time: 15 minutes
restart: 5 minutes
restart-count: 3

Command Modes

IPv4 VRF address family configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **neighbor maximum-prefix** command is configured to protect an individual peering session or all peering sessions. When this feature is enabled and the maximum prefix limit is exceeded, the router tears down the peering session, clears all routes that are learned from the peer, and then places the peer in a penalty state for the default or user-defined time period. After the penalty time period expires, normal peering is reestablished.



Note

In EIGRP, **neighbor** commands have been used traditionally to configure static neighbors. In the context of this feature, however, the **neighbor maximum-prefix** command can be used to configure the maximum prefix limit for both statically configured and dynamically discovered neighbors.

When configuring the **neighbor maximum-prefix** command to protect a single peering session, just the maximum prefix limit, percentage threshold, and warning only configuration options can be configured. Session dampening, restart, and reset timers are configured on a global basis.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	eigrp	read, write

Examples

Configuring the Maximum Prefix Limit for a Single Peer

The following example shows how to configure the maximum prefix limit for a single peer. The maximum limit is set to 1000 prefixes, and the warning threshold is set to 80 percent. When the maximum prefix limit is exceeded, the session with this peer is torn down, all routes learned from this peer are removed from the topology and routing tables, and this peer is placed in a penalty state for 5 minutes (default penalty value).

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp)# vrf vrf1
RP/0/RP0/CPU0:router(config-eigrp-vrf) address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-vrf-af)# neighbor 10.0.0.1 maximum-prefix 1000 80
```

Configuring the Maximum Prefix Limit for All Peers

The following example shows how to configure the maximum prefix limit for all peers. The maximum limit is set to 10,000 prefixes, the warning threshold is set to 90 percent, the restart timer is set to 4 minutes, a decay penalty is configured for the restart timer with the **dampened** keyword, and all timers are configured to be reset to 0 every 60 minutes. When the maximum prefix limit is exceeded, all peering sessions are torn down, all routes learned from all peers are removed from the topology and routing tables, and all peers are placed in a penalty state for 4 minutes (user-defined penalty value). A dampening exponential decay penalty is also applied.

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp)# vrf vrf1
RP/0/RP0/CPU0:router(config-eigrp-vrf) address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-vrf-af)# neighbor maximum-prefix 10000 90 dampened
reset-time 60 restart4
```

Related Commands	Command	Description
	clear eigrp neighbors	Deletes EIGRP and VRF neighbor entries from the appropriate tables.
	clear route	Deletes routes from the IP routing table.

R3.3 Beta Draft – Cisco Confidential Information

next-hop-self disable

To instruct the Enhanced Interior Gateway Routing Protocol (EIGRP) process to use the received next-hop value when advertising these routes, use the **next-hop-self disable** command in interface configuration mode. To instruct EIGRP to use the received next-hop rather than itself, use the **no** form of this command.

next-hop-self disable

no next-hop-self disable

Syntax Description

This command has no arguments or keywords.

Defaults

EIGRP always sets the IP next-hop value to be itself.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

EIGRP, by default, sets the IP next-hop value to be itself for routes that it is advertising, even when advertising those routes on the same interface from which learned them. To change this default, you must use the **next-hop-self disable** interface configuration command to instruct EIGRP to use the received next-hop value when advertising these routes. An exception to this guideline is if spoke-to-spoke dynamic tunnels are not wanted, then the **no next-hop-self** command is not needed.

Task ID

Task ID	Operations
eigrp	read, write

Examples

The following example shows how to change the default IP next-hop value and instruct EIGRP to use the received next-hop value:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp) address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-af)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-eigrp-af-if)# next-hop-self disable
```

R3.3 Beta Draft—Cisco Confidential Information

passive-interface (EIGRP)

To suppress routing updates on an Enhanced Interior Gateway Routing Protocol (EIGRP) interface, use the **passive-interface** command in interface configuration mode. To reenabel the sending of routing updates, use the no form of this command.

passive-interface

no passive-interface

Syntax Description This command has no arguments or keywords.

Defaults Routing updates are sent on the interface.

Command Modes Interface configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **passive-interface** command to disable the sending of routing updates on an interface. The particular subnet continues to advertise to other interfaces, and updates from other routers on that interface continue to be received and processed.

Task ID

Task ID	Operations
eigrp	read, write

Examples

The following example shows how to send EIGRP routing updates to all interfaces except Packet-over-SONET/SDH (POS) interface 0/1/0/0:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp) address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-af)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-eigrp-af-if)# passive-interface
```

R3.3 Beta Draft—Cisco Confidential Information

redistribute (EIGRP)

To inject routes from one routing domain into Enhanced Interior Gateway Routing Protocol (EIGRP), use the **redistribute** command in the appropriate configuration mode. To remove the **redistribute** command from the configuration file and restore the system to its default condition in which the software does not redistribute routes, use the **no** form of this command.

```
redistribute { { bgp | connected | isis | ospf | rip | static } [as-number | instance-name]}
[route-policy name]
```

```
no redistribute { bgp | connected | isis | ospf | rip | static } [as-number | instance-name]}
```

Syntax Description	
bgp	Distributes routes from the BGP protocol.
connected	Distributes routes that are established automatically by virtue of having enabled IP on an interface.
isis	Distributes routes from the IS-IS protocol.
ospf	Distributes routes from the OSPF protocol.
static	Redistributes IP static routes.
<i>as-number</i> <i>instance-name</i>	For the bgp keyword, an autonomous system number, which is a 16-bit decimal number. Range is 1 to 65535. For the isis keyword, an IS-IS instance name from which routes are to be redistributed. The value takes the form of a string. A decimal number can be entered, but it is stored internally as a string. For the ospf keyword, an OSPF instance name from which routes are to be redistributed. The value takes the form of a string. A decimal number can be entered, but it is stored internally as a string.
route-policy name	(Optional) Specifies the identifier of a configured policy. A policy is used to filter the importation of routes from this source routing protocol to EIGRP.

Defaults Route redistribution is disabled.

Command Modes Address family configuration
IPv4 VRF address family configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information

Redistributed routing information should always be filtered by the **route-policy** *name* keyword and argument. This filtering ensures that only those routes intended by the administrator are redistributed by EIGRP.

For information about routing policies, see *Routing Policy Commands on Cisco IOS XR Software* module of the *Cisco IOS XR Routing Command Reference*.

Task ID	Task ID	Operations
	eigrp	read, write

Examples

The following example shows how to cause BGP routes to be redistributed into an EIGRP autonomous system:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp) address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-af)# redistribute bgp 100
```

The following example shows how to redistribute the specified IS-IS process routes into an EIGRP autonomous system within a VPN routing and forwarding instance (VRF). The IS-IS routes are redistributed using route policy 3.

```
RP/0/RP0/CPU0:router(config)# router eigrp 109
RP/0/RP0/CPU0:router(config-eigrp)# vrf vpn-1
RP/0/RP0/CPU0:router(config-eigrp-vrf)# address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-vrf-af)# redistribute isis 108 route-policy 3
```

R3.3 Beta Draft—Cisco Confidential Information

redistribute maximum-prefix

To limit the number of prefixes redistributed into an Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the **redistribute maximum-prefix** command in IPv4 VRF address family configuration mode. To disable this function, use the **no** form of this command.

redistribute maximum-prefix *maximum* [*threshold*] [[**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] | [**warning-only**]]

no redistribute maximum-prefix *maximum* [*threshold*] [[**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] | [**warning-only**]]

Syntax Description		
<i>maximum</i>	Maximum number of prefixes that are redistributed into EIGRP under an address-family. The range is from 1 to 4294967295.	
	Note	The number of prefixes that can be configured is limited only by the available system resources on the router.
<i>threshold</i>	(Optional) Syslog warning messages are specified as a percentage of the maximum prefix limit that was exceeded. The prefix percentage number range is from 1 to 100. The default is 75 percent.	
restart <i>minutes</i>	(Optional) Configures a time period in which the router will not form adjacencies or accept redistributed routes from the RIB after the <i>maximum-prefix</i> limit has been exceeded. The value for the minutes argument is from 1 to 65535 minutes.	
restart-count <i>number</i>	(Optional) Configures the number of times a peering session can be automatically reestablished after the peering session has been torn down or after the redistribute route has been cleared and relearned because the maximum prefix limit has been exceeded.	
		
	Caution	After the restart count threshold has been crossed, you will need to enter the clear route * or clear eigrp neighbor command to reestablish normal peering, redistribution, or both.
reset-time <i>minutes</i>	(Optional) Configures the router to reset the restart count to 0 after the default or configured reset time period has expired. The value for the minutes argument is from 1 to 65535 minutes.	
dampened	(Optional) Configures a decay penalty to be applied to the restart time period each time the maximum prefix limit is exceeded. The half-life for the decay penalty is 150 percent of the default or user-defined restart time value in minutes.	
warning-only	(Optional) Configures the router to only generate syslog messages when the maximum prefix limit is reached, instead of suspending redistribution.	

Defaults

threshold: 75 percent
warning-only: disabled
reset-time: 15 minutes

R3.3 Beta Draft—Cisco Confidential Information

restart: 5 minutes
 restart-count: 3
 dampened: disabled

Command Modes

IPv4 VRF address family configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **redistribute maximum-prefix** command to configure limit prefixes learned through redistribution. When the maximum prefix limit is exceeded, all routes learned from the Routing Information Base (RIB) are discarded and redistribution is suspended for the default or user-defined time period. The maximum prefix limit that can be configured for redistributed prefixes is limited only by the available system resources on the router.

Task ID

Task ID	Operations
eigrp	read, write

Examples

The following example shows how to configure the maximum prefix limit for routes learned through redistribution. The maximum limit is set to 5000 prefixes, and the warning threshold is set to 95 percent. When the number of prefixes learned through redistribution reaches 4750 (95 percent of 5000), warning messages are displayed in the console. Because the **warning-only** keyword is configured, the topology and routing tables are not cleared and route redistribution is not placed in a penalty state.

```
RP/0/0/CPU0:router(config)# router eigrp 100
RP/0/0/CPU0:router(config-eigrp)# vrf vpn-1
RP/0/0/CPU0:router(config-eigrp-vrf)# address-family ipv4
RP/0/0/CPU0:router(config-eigrp-vrf-af)# redistribute maximum-prefix 5000 95 warning-only
```

Related Commands

Command	Description
clear eigrp neighbors	Deletes EIGRP and VPN neighbor entries from the appropriate table.
clear route	Deletes routes from the IP routing table.

R3.3 Beta Draft—Cisco Confidential Information

route-policy (EIGRP)

To apply a routing policy to updates advertised to or received from an Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor, use the **route-policy** command in the appropriate configuration mode. To disable applying routing policy to updates, use the **no** form of this command.

route-policy *route-policy-name* {**in** | **out**}

no route-policy *route-policy-name* {**in** | **out**}

Syntax Description

<i>route-policy-name</i>	Name of route policy.
in	Applies policy to inbound routes.
out	Applies policy to outbound routes.

Defaults

No policy is applied.

Command Modes

Address family configuration
IPv4 VRF address family configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **route-policy** command to specify a routing policy for an inbound or outbound route. The policy can be used to filter routes or modify route attributes. The **route-policy** command is used to define a policy.

Task ID

Task ID	Operations
eigrp	read, write

Examples

The following example shows how to apply the In-Ipv4 policy to inbound IP Version 4 (IPv4) routes from neighbor 172.20.1.1

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp) address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-af)# route-policy IN-IPv4 in
```

R3.3 Beta Draft—Cisco Confidential Information

router eigrp

To configure a routing process and enter router configuration mode for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **router eigrp** command in global configuration mode. To turn off the EIGRP routing process, use the **no** form of this command.

router eigrp *as-number*

no router eigrp *as-number*

Syntax Description	<i>as-number</i> (Optional) Autonomous system number. Range is from 1 to 65535.

Defaults	No routing process is defined.

Command Modes	Global

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	eigrp	read, write

Examples	The following example shows how to configure a routing process for EIGRP:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp)#
```

R3.3 Beta Draft—Cisco Confidential Information

router-id (EIGRP)

To configure a router ID for an Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the **router-id** command in the appropriate configuration mode. To cause the software to use the default method of determining the router ID, use the **no** form of this command.

router-id *router-id*

no router-id *router-id*

Syntax Description

<i>router-id</i>	32-bit router ID value specified in four-part, dotted-decimal notation.

Defaults

If this command is not configured, the router ID is the highest IP version 4 (IPv4) address for an interface on the router, with any loopback interface taking precedence.

Command Modes

Address family configuration
IPv4 VRF address family configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

It is good practice to use the **router-id** command to explicitly specify a unique 32-bit numeric value for the router ID. This action ensures that EIGRP can function regardless of the interface address configuration.

Task ID

Task ID	Operations
eigrp	read, write

Examples

The following example shows how to assign the IP address of 172.20.1.1 to the EIGRP process 1:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp) address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-af)# router-id 172.20.1.1
```

R3.3 Beta Draft—Cisco Confidential Information

show eigrp accounting

To display prefix accounting information for Enhanced Interior Gateway Routing Protocol (EIGRP) processes, use the **show eigrp accounting** command in EXEC mode.

```
show eigrp [vrf {vrf-name | all}] accounting [as-number]
```

Syntax Description

vrf {vrf-name all}	(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances.
as-number	(Optional) Autonomous system number. Range is from 1 to 65535.

Defaults

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
EIGRP	read

Examples

TBD

R3.3 Beta Draft—Cisco Confidential Information

show eigrp interfaces

To display information about interfaces configured for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show eigrp interfaces** command in EXEC mode.

show eigrp [**vrf** {*vrf-name* | **all**}] **interfaces** [*type instance*] [*as-number*] [**detail**]

Syntax Description		
vrf { <i>vrf-name</i> all }		(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances.
<i>type</i>		(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>instance</i>		(Optional) Either a physical interface instance or a virtual interface instance.
		Specifying these arguments removes the specified interface type from the neighbor table that all entries learned via this interface.
		- Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type.
		For more information about the syntax for the router, use the question mark (?) online help function.
<i>as-number</i>		(Optional) Autonomous system number. Range is from 1 to 65535.
detail		(Optional) Displays detailed EIGRP interface information.

Defaults This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show eigrp interfaces** command to determine on which interfaces EIGRP is active and learn information about EIGRP related to those interfaces.

If an interface is specified, only that interface is displayed. Otherwise, all interfaces on which EIGRP is running are displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all EIGRP processes are displayed.

Task ID

Task ID	Operations
EIGRP	read

Examples

TBD

Related Commands

Command	Description
show eigrp neighbors	Displays the neighbors discovered by EIGRP.

R3.3 Beta Draft—Cisco Confidential Information

show eigrp neighbors

To display the neighbors discovered by Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show eigrp neighbors** command in EXEC mode.

```
show eigrp [vrf {vrf-name | all}] neighbors [as-number] [detail] [interface-type interface-instance | static]
```

Syntax Description		
vrf { <i>vrf-name</i> all }		(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances.
<i>as-number</i>		(Optional) Autonomous system number. Range is from 1 to 65535.
detail		(Optional) Displays detailed EIGRP neighbor information.
<i>interface-type</i>		(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>		(Optional) Either a physical interface instance or a virtual interface instance.
		Specifying these arguments removes the specified interface type from the neighbor table that all entries learned via this interface.
		- Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type.
		For more information about the syntax for the router, use the question mark (?) online help function.
static		(Optional) Displays static routes.

Defaults This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

 show eigrp neighbors

R3.3 Beta Draft – Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
EIGRP	read

Examples

TBD

R3.3 Beta Draft—Cisco Confidential Information

show eigrp topology

To display entries in the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table, use the **show eigrp topology** command in EXEC mode.

show eigrp [**vrf** {*vrf-name* | **all**}] **topology** [*as-number* | [*ip-address mask*] [**active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors**]

Syntax Description		
vrf { <i>vrf-name</i> all }		(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances.
<i>as-number</i>		(Optional) Autonomous system number.
<i>ip-address</i>		(Optional) IP address in four-part, dotted-decimal notation.
<i>mask</i>		(Optional) Network mask specified in either of two ways: - Network mask can be a four-part, dotted decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit is a network address. - Network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are 1s, and the corresponding bits of the address are the network address.
active		(Optional) Displays only active entries in the EIGRP topology table.
all-links		(Optional) Displays all entries in the EIGRP topology table.
detail-links		(Optional) Displays detailed information for all entries in the EIGRP topology table.
pending		(Optional) Displays all entries in the EIGRP topology table that are waiting for an update from a neighbor or are waiting to reply to a neighbor.
summary		(Optional) Displays a summary of the EIGRP topology table.
zero-successors		(Optional) Displays available routes in the EIGRP topology table.

Command Modes	EXEC

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When the **show eigrp topology** command is used without any keywords or arguments, only routes that are feasible successors are displayed.

The **show eigrp topology** command can be used to determine Diffusing Update Algorithm (DUAL) states and to debug possible DUAL problems.

 show eigrp topology

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	EIGRP	read

Examples	TBD

R3.3 Beta Draft—Cisco Confidential Information

show eigrp traffic

To display the number of Enhanced Interior Gateway Routing Protocol (EIGRP) packets sent and received, use the **show eigrp traffic** command in EXEC mode.

```
show eigrp [vrf {vrf-name | all}] traffic [as-number]
```

Syntax Description	vrf {vrf-name all}	(Optional) Specifies a particular VPN routing and forwarding instance (VRF) or all VRF instances.
	as-number	(Optional) Autonomous system number.

Command Modes	EXEC

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	EIGRP	read

Examples	TBD

R3.3 Beta Draft—Cisco Confidential Information

site-of-origin (EIGRP)

To configure the Site of Origin (SoO) filtering on an Enhanced Interior Gateway Routing Protocol (EIGRP) interface, use the **site-of-origin** command in interface configuration mode. To disable SoO filtering on an interface, use the no form of this command.

site-of-origin {*as-number:number* | *ip-address:number*}

no site-of-origin {*as-number:number* | *ip-address:number*}

Syntax Description	as-number:	Autonomous system number. Range is from 1 to 65535.
		The colon is used to separate the autonomous system number and network number.
	number	Network number. Range is from 1 to 4294967295.
	ip-address:	IP address in four-part, dotted-decimal notation.
		The colon is used to separate the IP address and network number.

Defaults	No default behavior or values

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

TBD

Task ID	Task ID	Operations
	eigrp	read, write

Examples	The following example shows how to configure SoO filtering on an EIGRP interface:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp) address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-af)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-eigrp-af-if)# site-of-origin 10.0.0.1:20
```

R3.3 Beta Draft—Cisco Confidential Information

split-horizon disable (EIGRP)

To disable split horizon for an Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the **split-horizon disable** command in interface configuration mode. To enable split horizon, use the **no** form of this command.

split-horizon disable

no split-horizon disable

Syntax Description	This command has no arguments or keywords.

Defaults	Split horizon is enabled for an EIGRP process.

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

TBD

Task ID	Task ID	Operations
	eigrp	read, write

Examples	The following example shows how to disable split horizon on a Packet-over-SONET/SDH (POS) link:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp) address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-af)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-eigrp-af-if)# split-horizon disable
```

R3.3 Beta Draft—Cisco Confidential Information

stub (EIGRP)

To configure a router as a stub for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **stub** command in the appropriate configuration mode. To disable this function, use the **no** form of this command.

```
stub [receive-only | {[connected] [redistributed] [static] [summary]}]
```

```
no stub [receive-only | {[connected] [redistributed] [static] [summary]}]
```

Syntax Description

receive-only	(Optional) Sets the router as a receive-only neighbor.
connected	(Optional) Advertises connected routes.
redistributed	(Optional) Advertises redistributed routes from other protocols and autonomous systems.
static	(Optional) Advertises static routes.
summary	(Optional) Advertises summary routes.

Defaults

Stub routing is disabled.
When stub routing is specified, connected and summary routes are advertised by default.

Command Modes

Address family configuration
IPv4 VRF address family configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **stub** command to configure a router as a stub in which the router directs all IP traffic to a distribution router.

The **stub** command can be modified with several options, and these options can be used in any combination except for the **receive-only** keyword.

The **receive-only** keyword restricts the router from sharing any of its routes with any other router in that EIGRP autonomous system and does not permit any other option to be specified because it prevents any type of route from being sent. The four other optional keywords (**connected**, **static**, **summary**, and **redistributed**) can be used in any combination but cannot be used with the **receive-only** keyword. If any of these four keywords is used with the **stub** command, only the route types specified by the particular keyword or keywords are sent. Route types specified by the nonused keyword or keywords are not sent.

R3.3 Beta Draft—Cisco Confidential Information

The **connected** keyword permits EIGRP stub routing to send connected routes. If the connected routes are not covered by a network statement, it may be necessary to redistribute connected routes with the **redistribute connected** command under the EIGRP process. This option is enabled by default.

The **static** keyword permits EIGRP stub routing to send static routes. Without the configuration of this option, EIGRP does not send any static routes, including internal static routes that normally would be automatically redistributed. You may still need to redistribute static routes with the **redistribute static** command.

The **summary** keyword permits EIGRP stub routing to send summary routes. Summary routes can be created manually with the **summary address** command or automatically at a major network border router with the **auto-summary** command enabled. This option is enabled by default.

The **redistributed** keyword permits EIGRP stub routing to send other routing protocols and autonomous systems. Without the configuration of this option, EIGRP does not advertise redistributed routes.

Task ID	Task ID	Operations
	eigrp	read, write

Examples

The following example shows how to configure the router as a stub that advertises connected and summary routes:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp) address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-af)# stub
```

The following example shows how to configure the router as a receive-only neighbor (connected, summary, and static routes are not sent):

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp) address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-af)# stub receive-only
```

Related Commands	Command	Description
	redistribute (EIGRP)	Redistributes routes from one routing domain into EIGRP.
	summary-address (EIGRP)	Configures a summary aggregate address for the specified EIGRP interface.
	auto-summary (EIGRP)	Allows automatic summarization of subnet routes into network-level routes for an EIGRP process.

R3.3 Beta Draft—Cisco Confidential Information

summary-address (EIGRP)

To configure a summary aggregate address for the specified Enhanced Interior Gateway Routing Protocol (EIGRP) interface, use the **summary-address** command in interface configuration mode. To disable a configuration, use the **no** form of this command.

summary-address *ip-address* [/length | mask] [admin-distance]

no summary-address

Syntax Description	<i>ip-address</i>	The IP address argument specifies the summary IP address to apply to an interface in four-part, dotted-decimal notation.
	<i>/length</i>	Prefix length, which can be indicated as a slash (/) and number. For example, /8 indicates that the first eight bits in the IP prefix are network bits. If <i>length</i> is used, the slash is required.
	<i>mask</i>	IP address mask.
	<i>admin-distance</i>	(Optional) Administrative distance. A value from 1 to 255.

Defaults

An administrative distance of 5 is applied to EIGRP summary routes.
 EIGRP automatically summarizes to the network level, even for a single host route.
 No summary addresses are predefined.
 The default administrative distance metric for EIGRP is 90.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **summary-address** command is used to configure interface-level address summarization. EIGRP summary routes are given an administrative distance of 5. The administrative distance is used to advertise a summary without installing it in the routing table.

By default, EIGRP summarizes subnet routes to the network level. The **no auto-summary** command can be entered to configure subnet level summarization.

Task ID

Task ID	Operations
eigrp	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure an administrative distance of 95 on an EIGRP interface for the 192.168.0.0/16 summary address:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1  
RP/0/RP0/CPU0:router(config-eigrp) address-family ipv4  
RP/0/RP0/CPU0:router(config-eigrp-af)# interface pos 0/1/0/0  
RP/0/RP0/CPU0:router(config-eigrp-af-if)# summary-address 192.168.0.0/16 95
```

Related Commands

Command	Description
auto-summary (EIGRP)	Allows automatic summarization of subnet routes into network-level routes for an EIGRP process.

R3.3 Beta Draft—Cisco Confidential Information

timers active-time

To adjust the Enhanced Interior Gateway Routing Protocol (EIGRP) routing wait time, use the **timers active-time** command in the appropriate configuration mode. To disable this function, use the **no** form of the command.

timers active-time [*time-limit* | **disabled**]

no timers active-time

Syntax Description	<i>time-limit</i>	Active time limit (in minutes). The range is from 1 to 4294967295 minutes.
	disabled	Disables the timers and permits the routing wait time to remain active indefinitely.

Defaults	Disabled

Command Modes	Address family configuration IPv4 VRF address family configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the timers active-time command to control the time the router waits (after query is sent) before declaring the route to be in the stuck in active (SIA) state.

Task ID	Task ID	Operations
	eigrp	read, write

Examples	The following example shows how to configure an indefinite routing wait time on the specified EIGRP route: <pre>RP/0/RP0/CPU0:router(config)# router eigrp 1 RP/0/RP0/CPU0:router(config-eigrp) address-family ipv4 RP/0/RP0/CPU0:router(config-eigrp-af)# timers active-time disabled</pre>

R3.3 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show eigrp topology	Displays entries in the EIGRP topology table.

R3.3 Beta Draft—Cisco Confidential Information**timers nsf route-hold (EIGRP)**

To set the timer that determines how long an NSF-aware Enhanced Interior Gateway Routing Protocol (EIGRP) router holds routes for an inactive peer, use the **timers nsf route-hold** command in the appropriate configuration mode. To return the route hold timer to the default value, use the **no** form of this command.

timers nsf route-hold *seconds*

no timers nsf route-hold

Syntax Description	<i>seconds</i> Time, in seconds, that EIGRP holds routes for an inactive peer. Range is from 20 to 300 seconds.					
Defaults	EIGRP NSF awareness is enabled. <i>seconds</i> : 240					
Command Modes	Address family configuration IPv4 VRF address family configuration					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>Release 3.3</td><td>This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.</td></tr></table>		Release	Modification	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release	Modification					
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.					
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the timers nsf route-hold command to set the maximum period of time that the NSF-aware router holds known routes for an NSF-capable neighbor during a switchover operation or a well-known failure condition. The route hold timer is configurable so that you can tune network performance and avoid undesired effects, such as "black holing" routes if the switchover operation takes too much time. When this timer expires, the NSF-aware router scans the topology table and discards any stale routes, allowing EIGRP peers to find alternate routes instead of waiting during a long switchover operation.					
Task ID	<table><tr><th>Task ID</th><th>Operations</th></tr><tr><td>eigrp</td><td>read, write</td></tr></table>		Task ID	Operations	eigrp	read, write
Task ID	Operations					
eigrp	read, write					

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to set the route hold timer value for an NSF-aware router to 2 minutes (120 seconds):

```
RP/0/RP0/CPU0:router(config)# router eigrp 1  
RP/0/RP0/CPU0:router(config-eigrp) address-family ipv4  
RP/0/RP0/CPU0:router(config-eigrp-af)# timers nsf route-hold 120
```

R3.3 Beta Draft—Cisco Confidential Information

variance

To control load balancing in an Enhanced Interior Gateway Routing Protocol (EIGRP)-based internetwork, use the **variance** command in the appropriate configuration mode. To reset the variance to the default value, use the **no** form of this command.

variance *multiplier*

no variance

Syntax Description	multiplierMetric value used for load balancing. Range is from 1 to 128.					
Defaults	multiplier: 1 (equal-cost load balancing)					
Command Modes	Address family configuration IPv4 VRF address family configuration					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>Release 3.3</td><td>This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.</td></tr></table>		Release	Modification	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release	Modification					
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.					
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the variance command to set a variance on the EIGRP router so that the router can determine the feasibility of a potential route. A route is feasible if the next router in the path is closer to the destination than the current router and the metric for the entire path is within the variance. Only paths that are feasible can be used for load balancing and included in the routing table. If the following two conditions are met, the route is considered feasible and can be added to the routing table: 1. The local best metric must be greater than the metric learned from the next router. 2. The multiplier times the local best metric for the destination must be greater than or equal to the metric through the next router.					
Task ID	<table><tr><th>Task ID</th><th>Operations</th></tr><tr><td>eigrp</td><td>read, write</td></tr></table>		Task ID	Operations	eigrp	read, write
Task ID	Operations					
eigrp	read, write					

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to set a variance of 4:

```
RP/0/RP0/CPU0:router(config)# router eigrp 1  
RP/0/RP0/CPU0:router(config-eigrp) address-family ipv4  
RP/0/RP0/CPU0:router(config-eigrp-af)# variance 4
```

R3.3 Beta Draft—Cisco Confidential Information**vrf (EIGRP)**

To define a VPN routing and forwarding (VRF) instance and enter VRF configuration mode, use the **vrf** command in router configuration mode. To remove a VRF instance, use the **no** form of this command.

vrf *vrf-name*

no vrf *vrf-name*

Syntax Description	<i>vrf-name</i> VPN routing and forwarding instance.	
Defaults	No VRFs are defined. No import or export lists are associated with a VRF. No route maps are associated with a VRF.	
Command Modes	Router configuration	
Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .	
	Use the vrf command to configure a VRF instance. A VRF instance is a collection of VPN routing and forwarding tables maintained at the provider edge (PE) router.	
	From VRF configuration mode, you must enter address family configuration mode and then issue commands, such as the auto-summary command.	
Task ID	Task ID	Operations
	eigrp	read, write

Examples The following example shows how to enter IPv4 VRF address family configuration mode and identify EIGRP commands that can be issued from that mode.

```
RP/0/RP0/CPU0:router(config)# router eigrp 1
RP/0/RP0/CPU0:router(config-eigrp)# vrf vpn-1
RP/0/RP0/CPU0:router(config-eigrp-vrf)# address-family ipv4
RP/0/RP0/CPU0:router(config-eigrp-vrf-af)# ?
```

auto-summary	Auto summarisation
autonomous-system	Set the autonomous system of VRF
commit	Commit the configuration changes to running

R3.3 Beta Draft—Cisco Confidential Information

default-information	Handling of default route
default-metric	Set metric of redistributed routes
describe	Describe a command without taking real actions
distance	Set distance for EIGRP routes
do	Run an exec command
exit	Exit from this submode
interface	EIGRP interface configuration submode
log-neighbor-changes	Enable/Disable EIGRP neighbor logging
log-neighbor-warnings	Enable/Disable EIGRP neighbor warnings
maximum-paths	Maximum paths
maximum-prefix	Maximum number of IP prefixes acceptable in aggregate
metric	Modify EIGRP routing metrics and parameters
neighbor	Neighbor prefix limits configuration
no	Negate a command or set its defaults
redistribute	Redistribute another protocol
route-policy	Configure inbound/outbound policies
router-id	Set router ID
show	Show contents of configuration
stub	EIGRP stub
timers	Configure EIGRP timers
variance	Control load balancing variance

R3.3 Beta Draft – Cisco Confidential Information

IS-IS Commands on Cisco IOS XR Software

Beta Draft Cisco Confidential Information

This chapter describes the commands used to configure and monitor the Intermediate System-to-Intermediate System (IS-IS) protocol.

For detailed information about IS-IS concepts, configuration tasks, and examples, see the *Implementing IS-IS on Cisco IOS XR Software* configuration guide.

R3.3 Beta Draft—Cisco Confidential Information

address-family (IS-IS)

To enter address family configuration mode for configuring Intermediate System-to-Intermediate System (IS-IS) routing that use standard IP Version 4 (IPv4) and IP Version 6 (IPv6) address prefixes, use the **address-family** command in router configuration or interface configuration mode. To disable address family configuration mode, use the **no** form of this command.

address-family {ipv4 | ipv6} [unicast]

no address-family {ipv4 | ipv6} [unicast]

Syntax Description

ipv4	Specifies IPv4 address prefixes.
ipv6	Specifies IPv6 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.

Defaults

An address family is not specified.

Command Modes

Router configuration
Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **address family** command to place the router or interface in address family configuration mode. In router address family configuration mode you can configure routing that uses standard IPv4 or IPv6 address prefixes. In interface address family configuration mode you can alter interface parameters for IPv4 or IPv6.

An address family must be specified to configure parameters that apply on an individual address family basis or that pertain to a single address family.

Task ID

Task ID	Operations
isis	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure the IS-IS router process with IPv6 unicast address prefixes:

```
RP/0/RP0/CPU0:router(config)# router isis isp  
RP/0/RP0/CPU0:router(config-isis)# address-family ipv6 unicast  
RP/0/RP0/CPU0:router(config-isis-af)#
```

R3.3 Beta Draft—Cisco Confidential Information

adjacency-check disable

To suppress Intermediate System-to-Intermediate System (IS-IS) IP Version 4 (IPv4) or IP Version 6 (IPv6) protocol-support consistency checks performed on hello packets, use the **adjacency-check disable** command in router address family configuration mode. To remove this function, use the **no** form of this command.

adjacency-check disable

no adjacency-check disable

Syntax Description This command has no arguments or keywords.

Defaults IS-IS checks that hello packets contain a subnet-matching IPv4 or IPv6 address.

Command Modes Router address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

IS-IS performs consistency checks on hello packets and forms an adjacency only with a neighboring router that supports the same set of protocols. A router running IS-IS for both IPv4 and IPv6 does not form an adjacency with a router running IS-IS for IPv4 only.

Use the **adjacency-check disable** command to suppress the consistency checks for IPv6 IS-IS and allow an IPv4 IS-IS router to form an adjacency with a router running IPv4 IS-IS and IPv6. IS-IS never forms an adjacency between a router running IPv4 IS-IS only and a router running IPv6 only.

In addition, the **adjacency-check disable** command suppresses the IPv4 subnet consistency check and allows IS-IS to form an adjacency with other routers regardless of whether they have an IPv4 subnet in common. In multitopology mode, the IPv4 subnet consistency check is automatically suppressed.

Task ID

Task ID	Operations
isis	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how the network administrator introduces IPv6 into an existing IPv4 IS-IS network and ensures that the checking of hello packet checks from adjacent neighbors is disabled until all neighbor routers are configured to use IPv6:

```
RP/0/RP0/CPU0:router(config)# router isis isp  
RP/0/RP0/CPU0:router(config-isis)# address-family ipv6  
RP/0/RP0/CPU0:router(config-isis-af)# adjacency-check disable
```

R3.3 Beta Draft—Cisco Confidential Information

circuit-type

To configure the type of adjacency used for the Intermediate System-to-Intermediate System (IS-IS) protocol, use the **circuit-type** command in interface configuration mode. To reset the circuit type to Level 1 and Level 2, use the **no** form of this command.

circuit-type {level-1 | level-1-2 | level-2-only }

no circuit-type

Syntax Description

level-1	Establishes only Level 1 adjacencies over an interface.
level-1-2	Establishes both Level 1 and Level 2 adjacencies, if possible.
level-2-only	Establishes only Level 2 adjacencies over an interface.

Defaults

Default adjacency types are both Level 1 and Level 2 adjacencies.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Adjacencies may not be established even if allowed by the **circuit-type** command. The proper way to establish adjacencies is to configure a router as a Level 1, Level 1 and Level 2, or Level 2-only system using the **is-type** command. Only on networking devices that are between areas (Level 1 and Level 2 networking devices) should you configure some interfaces to be Level 2-only to prevent wasting bandwidth by sending out unused Level 1 hello packets. Remember that on point-to-point interfaces, the Level 1 and Level 2 hello packets are in the same packet.

Task ID

Task ID	Operations
isis	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure a Level 1 adjacency with its neighbor on Packet-over-SONET (POS) interface 0/2/0/0 and Level 2 adjacencies with all Level 2-capable routers on POS interface 0/5/0/2:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# is-type level-1-2
RP/0/RP0/CPU0:router(config-isis)# interface POS0/2/0/0
RP/0/RP0/CPU0:router(config-isis-if)# circuit-type level-1
RP/0/RP0/CPU0:router(config-isis-if)# exit
RP/0/RP0/CPU0:router(config-isis)# interface POS0/5/0/2
RP/0/RP0/CPU0:router(config-isis-if)# circuit-type level-2-only
```

In this example, only Level 2 adjacencies are established because the **is-type** command is configured:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# is-type level-2-only
RP/0/RP0/CPU0:router(config-isis)# interface POS0/2/0/0
RP/0/RP0/CPU0:router(config-isis-if)# circuit-type level-1-2
```

Related Commands

Command	Description
is-type	Configures the routing level for an instance of the IS-IS routing process.
net	Configures an IS-IS NET for the routing process.

R3.3 Beta Draft—Cisco Confidential Information

clear isis process

To clear the link-state packet (LSP) database and adjacency database sessions for an Intermediate System-to-Intermediate System (IS-IS) instance or all IS-IS instances, use the **clear isis process** command in EXEC mode.

clear isis [**instance** *instance-id*] **process**

Syntax Description

instance *instance-id* (Optional) Specifies IS-IS sessions for the specified IS-IS instance only.

- The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **clear isis process** command without any keyword to clear all the IS-IS instances. Add the **instance** *instance-id* keyword and argument to clear the specified IS-IS instance.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows the IS-IS LSP database and adjacency sessions being cleared for instance 1:

```
RP/0/RP0/CPU0:router# clear isis instance 1 process
```

R3.3 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show isis database	Displays the IS-IS link-state database.
	show isis neighbors	Displays information about IS-IS neighbors.

R3.3 Beta Draft—Cisco Confidential Information

clear isis route

To clear the Intermediate System-to-Intermediate System (IS-IS) routes in a topology, use the **clear isis route** command in EXEC mode.

clear isis [**instance** *instance-id*] {**afi-all** | **ipv4 unicast** | **ipv6 unicast**} **route**

Syntax Description

instance <i>instance-id</i>	(Optional) Specifies IS-IS sessions for the specified IS-IS instance only. The <i>instance-id</i> argument is the instance identifier (alphanumeric) defined by the router isis command.
afi-all	Specifies IP Version 4 (IPv4) and IP Version 6 (IPv6) address prefixes.
ipv4 unicast	Specifies IPv4 unicast address prefixes.
ipv6 unicast	Specifies IPv6 unicast address prefixes.

Defaults

No default behavior or value

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The all keyword was changed to afi-all .
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **clear isis route** command to clear the routes from the specified topology or all routes in all topologies if no topology is specified.

Task ID

Task ID	Operations
isis	execute
rib	read, write
basic-services	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to clear the routes with IPv4 unicast address prefixes:

```
RP/0/RP0/CPU0:router# clear isis ipv4 unicast route
```

Related Commands

Command	Description
show isis database	Displays the IS-IS link-state database.
show isis neighbors	Displays information about IS-IS neighbors.

R3.3 Beta Draft—Cisco Confidential Information

clear isis statistics

To clear the Intermediate System-to-Intermediate System (IS-IS) statistics, use the **clear isis statistics** command in EXEC mode.

clear isis [**instance** *instance-id*] **statistics** [*interface-type interface-instance*]

Syntax Description

instance <i>instance-id</i>	(Optional) Clears IS-IS sessions for the specified IS-IS instance only. The <i>instance-id</i> argument is the instance identifier (alphanumeric) defined by the router isis command.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance as follows: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.3	No modification.

R3.3 Beta Draft – Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **clear isis statistics** command to clear the information displayed by the **show isis statistics** command.

Task ID

Task ID	Operations
isis	execute
rib	read, write
basic-services	read, write

Examples

The following example shows the IS-IS statistics for a specified interface being cleared:

```
RP/0/RP0/CPU0:router# clear isis instance 23 statistics
```

Related Commands

Command	Description
show isis statistics	Displays the IS-IS statistics.

R3.3 Beta Draft—Cisco Confidential Information

csnp-interval

To configure the interval at which periodic complete sequence number PDUs (CSNPs) packets are sent on broadcast interfaces, use the **csnp-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

csnp-interval *seconds* [**level** { **1** | **2** }]

no csnp-interval

Syntax Description

<i>seconds</i>	Interval (in seconds) of time between transmission of CSNPs on multiaccess networks. This interval applies only for the designated router. Range is 0 to 65535 seconds.
level { 1 2 }	(Optional) Specifies the interval of time between transmission of CSNPs for Level 1 or Level 2 independently.

Defaults

seconds: 10 seconds
Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **csnp-interval** command applies only to the designated router (DR) for a specified interface. Only DRs send CSNP packets to maintain database synchronization. The CSNP interval can be configured independently for Level 1 and Level 2.

Use of the **csnp-interval** command on point-to-point subinterfaces makes sense only in combination with the IS-IS mesh-group feature.



Note

It is unlikely that you will ever need to change the default value of this command.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	isis	execute
	rib	read, write
	basic-services	read, write

Examples

The following example shows how to set the CSNP interval for Level 1 to 30 seconds:

```
RP/0/RP0/CPU0:router(config)# router isis isp  
RP/0/RP0/CPU0:router(config-isis)# interface POS0/0/2/0  
RP/0/RP0/CPU0:router(config-isis-if)# csnp-interval 30 level 1
```

R3.3 Beta Draft—Cisco Confidential Information

default-information originate (IS-IS)

To generate a default route into an Intermediate System-to-Intermediate System (IS-IS) routing domain, use the **default-information originate** command in router address family configuration mode. To remove the **default-information originate** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

default-information originate [**route-policy** *route-policy-name*]

no default-information originate [**route-policy** *route-policy-name*]

Syntax Description

route-policy	(Optional) Defines the conditions for the default route.
<i>route-policy-name</i>	(Optional) Meaningful name for the route map.

Defaults

A default route is not generated into an IS-IS routing domain.

Command Modes

Router address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	The route-map <i>map-name</i> keyword and argument were changed to route-policy <i>route-policy-name</i> .

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If a router configured with the **default-information originate** command has a route to 0.0.0.0 in the routing table, IS-IS originates an advertisement for 0.0.0.0 in its link-state packets (LSPs).

Without a route policy, the default is advertised only in Level 2 LSPs. For Level 1 routing, there is another process to find the default route, which is to look for the closest Level 1 and Level 2 router. The closest Level 1 and Level 2 router can be found by looking at the attached-bit (ATT) in Level 1 LSPs.

A route policy can be used for two purposes:

- To make the router generate the default route in its Level 1 LSPs.
- To advertise 0/0 conditionally.

Task ID

Task ID	Operations
isis	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to generate a default external route into an IS-IS domain:

```
RP/0/RP0/CPU0:router(config)# router isis isp  
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast  
RP/0/RP0/CPU0:router(config-isis-af)# default-information originate
```

Related Commands

Command	Description
redistribute (IS-IS)	Redistributes routes from one IS-IS instance into another instance.
show isis database	Displays the IS-IS link-state database.

R3.3 Beta Draft—Cisco Confidential Information

disable (IS-IS)

To disable the Intermediate System-to-Intermediate System (IS-IS) protocol on a specified interface, use the **disable** command in interface address family configuration mode. To remove this function, use the **no** form of this command.

disable

no disable

Syntax Description	This command has no arguments or keywords.	
Defaults	IS-IS protocol is enabled.	
Command Modes	Interface address family configuration	
Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
	Release 3.3	No modification.
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .	
Task ID	Task ID	Operations
	isis	read, write
Examples	The following example shows how to disable the IS-IS protocol being disabled for IPv4 unicast on Packet-over-SONET (POS) interface 0/1/0/1: <pre>RP/0/RP0/CPU0:router(config)# router isis isp RP/0/RP0/CPU0:router(config-isis)# interface POS0/1/0/1 RP/0/RP0/CPU0:router(config-isis-if)# address-family ipv4 unicast RP/0/RP0/CPU0:router(config-isis-if-af)# disable</pre>	

R3.3 Beta Draft—Cisco Confidential Information

distance (IS-IS)

To define the administrative distance assigned to routes discovered by the Intermediate System-to-Intermediate System (IS-IS) protocol, use the **distance** command in router address family configuration mode. To remove the **distance** command from the configuration file and restore the system to its default condition in which the software removes a distance definition, use the **no** form of this command.

distance *weight* [*address/prefix-length* [*route-list-name*]]

no distance *weight* [*address/prefix-length* [*route-list-name*]]

Syntax Description

<i>weight</i>	Administrative distance to be assigned to IS-IS routes. Range is 1 to 255.
<i>address/prefix-length</i>	(Optional) The <i>address</i> argument specifies the IP address in four-part, dotted-decimal notation. The <i>prefix-length</i> argument specifies the length of the IP prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value. Range is 0 to 32 for IPv4 addresses and 0 to 128 for IPv6 addresses.
<i>route-list-name</i>	(Optional) List of routes to which administrative distance applies.

Defaults

weight: 115

Command Modes

Router address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

An administrative distance is an integer from 1 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means that the routing information source cannot be trusted at all and should be ignored. Weight values are subjective; no quantitative method exists for choosing weight values.

R3.3 Beta Draft—Cisco Confidential Information

Use the **distance** command to configure the administrative distances applied to IS-IS routes when they are inserted into the Routing Information Base (RIB), and influence the likelihood of these routes being preferred over routes to the same destination addresses discovered by other protocols.

The *address/prefix-length* argument defines to which source router the distance applies. In other words, each IS-IS route is advertised by another router, and that router advertises an address that identifies it. The **distance** command applies to the routes advertised by routers whose address matches the specified prefix. The *route-list-name* argument can then be used to refine this further so that the **distance** command affects only specific routes.

Task ID	Task ID	Operations
	isis	read, write

Examples

The following example gives a distance of 10 to all routes to 2.0.0.0/8 and 3.0.0.0/8 (or more specific prefixes) that are advertised by routers whose ID is contained in 1.0.0.0/8. It gives a distance of 80 to all other routes.

```
RP/0/RP0/CPU0:router(config)# ipv4 prefix-list target_routes
RP/0/RP0/CPU0:router(config-ipv4_pfx)# permit 2.0.0.0/8
RP/0/RP0/CPU0:router(config-ipv4_pfx)# permit 3.0.0.0/8
RP/0/RP0/CPU0:router(config-ipv4_pfx)# deny 0.0.0.0/0
RP/0/RP0/CPU0:router(config-ipv4_pfx)# exit
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# distance 10 1.0.0.0/8 target_routes
RP/0/RP0/CPU0:router(config-isis-af)# distance 80
```

Related Commands	Command	Description
	router isis	Configures the IS-IS routing protocol and specifies an IS-IS instance.
	show isis protocol	Displays summary information about the IS-IS instance.

R3.3 Beta Draft—Cisco Confidential Information

hello-interval (IS-IS)

To specify the length of time between hello packets sent by the Intermediate System-to-Intermediate System (IS-IS) protocol software, use the **hello-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

hello-interval *seconds* [**level** {**1** | **2**}]

no hello-interval *seconds* [**level** {**1** | **2**}]

Syntax Description

<i>seconds</i>	Integer value (in seconds) for the length of time between hello packets. By default, a value three times the hello interval <i>seconds</i> is advertised as the <i>hold time</i> in the hello packets sent. (That multiplier of three can be changed by using the hello-multiplier command.) With smaller hello intervals, topological changes are detected more quickly, but there is more routing traffic. Range is 1 to 65535 seconds.
level { 1 2 }	(Optional) Specifies the hello interval for Level 1 and Level 2 independently. For broadcast interfaces only.

Defaults

seconds: 10 seconds
Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The hello interval can be configured independently for Level 1 and Level 2, except on serial point-to-point interfaces. (Because only a single type of hello packet is sent on serial links, it is independent of Level 1 or Level 2.) Configuring Level 1 and Level 2 independently is used on Switched Multimegabit Data Service (SMDS) multiaccess networks or LAN interfaces.



Note

A shorter hello interval gives earlier convergence, but increases bandwidth and CPU usage. It might also add to instability in the network.

R3.3 Beta Draft—Cisco Confidential Information

A slower hello interval saves bandwidth and CPU. Especially when used in combination with a higher hello multiplier, this strategy may increase overall network stability.

We recommend that you tune the hello interval and hello multiplier on point-to-point interfaces rather than on LAN interfaces.

For point-to-point links, IS-IS sends only a single hello for Level 1 and Level 2, making the **level** keyword meaningless on point-to-point links. To modify hello parameters for a point-to-point interface, omit the **level** keyword.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure 10-GB Ethernet interface 0/6/0/0 to advertise hello packets every 5 seconds for Level 1 topology routes. This situation causes more traffic than configuring a longer interval, but topological changes are detected more quickly.

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# interface TenGigE 0/6/0/0
RP/0/RP0/CPU0:router(config-isis-if)# hello-interval 5 level 1
```

Related Commands

Command	Description
hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the router should declare the adjacency as down.

R3.3 Beta Draft—Cisco Confidential Information

hello-multiplier

To specify the number of Intermediate System-to-Intermediate System (IS-IS) hello packets a neighbor must miss before the router should declare the adjacency as down, use the **hello-multiplier** command in interface configuration mode. To restore the default value, use the **no** form of this command.

hello-multiplier *multiplier* [**level** {**1** | **2**}]

no hello-multiplier *multiplier* [**level** {**1** | **2**}]

Syntax Description

<i>multiplier</i>	Advertised hold time in IS-IS hello packets is set to the hello multiplier times the hello interval. Range is 3 to 1000. Neighbors declare an adjacency to this down router after not having received any IS-IS hello packets during the advertised hold time. The hold time (and thus the hello multiplier and the hello interval) can be set on an individual interface basis, and can be different between different networking devices in one area. Using a smaller hello multiplier gives fast convergence, but can result in more routing instability. Increase the hello multiplier to a larger value to help network stability when needed. Never configure a hello multiplier to a value lower than the default value of 3.
level { 1 2 }	(Optional) Specifies the hello multiplier independently for Level 1 or Level 2 adjacencies.

Defaults

multiplier: 3
Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The “holding time” carried in an IS-IS hello packet determines how long a neighbor waits for another hello packet before declaring the neighbor to be down. This time determines how quickly a failed link or neighbor is detected so that routes can be recalculated.

R3.3 Beta Draft—Cisco Confidential Information

Use the **hello-multiplier** command in circumstances where hello packets are lost frequently and IS-IS adjacencies are failing unnecessarily. You can raise the hello multiplier and lower the hello interval (**hello-interval (IS-IS)** command) correspondingly to make the hello protocol more reliable without increasing the time required to detect a link failure.

On point-to-point links, there is only one hello for both Level 1 and Level 2. Therefore, configuring different hello multipliers is useful only for multiaccess networks, which are not currently supported. Separate Level 1 and Level 2 hello packets are also sent over nonbroadcast multiaccess (NBMA) networks in multipoint mode, such as X.25, Frame Relay, and ATM. However, we recommend that you run IS-IS over point-to-point subinterfaces over WAN NBMA media.

Task ID	Task ID	Operations
	isis	read, write

Examples

The following example shows how the network administrator wants to increase network stability by making sure an adjacency goes down only when many (ten) hello packets are missed. The total time to detect link failure is 60 seconds. This strategy ensures that the network remains stable, even when the link is fully congested.

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# interface POS0/2/0/1
RP/0/RP0/CPU0:router(config-isis-if)# hello-interval 6
RP/0/RP0/CPU0:router(config-isis-if)# hello-multiplier 10
```

Related Commands	Command	Description
	hello-interval (IS-IS)	Specifies the length of time between hello packets that the software sends.

R3.3 Beta Draft—Cisco Confidential Information

hello-padding

To configure padding on Intermediate System-to-Intermediate System (IS-IS) hello protocol data units (IIH PDUs) for all IS-IS interfaces on the router, use the **hello-padding** command in interface configuration mode. To suppress padding, use the **no** form of this command.

hello-padding {**disable** | **sometimes**} [**level** {**1** | **2**}]

no hello-padding

Syntax Description	disable	Suppresses hello padding.
	sometimes	Enables hello padding during adjacency formation only.
	level { 1 2 }	(Optional) Specifies hello padding for Level 1 or Level 2 independently.

Defaults	Hello padding is enabled.

Command Modes	Interface configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You might want to suppress hello padding to conserve network resources. The lower the circuit speed, the higher the percentage of padding overhead. Before suppressing the hello padding, you should know your physical and data link layer configurations and have control over them, and also know your router configuration at the network layer.

For point-to-point links, IS-IS sends only a single hello for Level 1 and Level 2, making the **level** keyword meaningless on point-to-point links. To modify hello parameters for a point-to-point interface, omit the **level** keyword.

Task ID	Task ID	Operations
	isis	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to suppress IS-IS hello padding over local area network (LAN) circuits for interface POS 0/2/0/1:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# interface POS0/2/0/1
RP/0/RP0/CPU0:router(config-isis-if)# hello-padding disable
```

Related Commands

Command	Description
show isis interface	Displays information about the IS-IS interface.

R3.3 Beta Draft—Cisco Confidential Information

hello-password

To configure the authentication password for an Intermediate System-to-Intermediate System (IS-IS) interface, use the **hello-password** command in interface configuration mode. To disable authentication, use the **no** form of this command.

hello-password { **hmac-md5** | **text** } { **clear** | **encrypted** } *password* [**level** { **1** | **2** }] [**send-only**]

no hello-password

Syntax Description

hmac-md5	Specifies that the password uses HMAC-MD5 authentication.
text	Specifies that the password uses clear text password authentication.
clear	Specifies that the password be unencrypted.
encrypted	Specifies that the password be encrypted using a two-way algorithm.
<i>password</i>	Authentication password you assign for an interface.
level { 1 2 }	(Optional) Specifies the authentication password for Level 1 or Level 2 independently.
send-only	(Optional) Adds passwords to IS-IS hello protocol data units (IIH PDUs) when they are sent. Does not check for authentication in received IIH PDUs.

Defaults

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The clear and encrypted keywords replaced the 0 and 7 keywords, and the hmac-md5 , text , and send-only keywords were added.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When a **text** password is configured, it is exchanged as clear text. Therefore, the **hello-password** command provides limited security.

When an **hmac-md5** password is configured, the password is never sent over the network and is instead used to calculate a cryptographic checksum to ensure the integrity of the exchanged data.

R3.3 Beta Draft—Cisco Confidential Information

For point-to-point links, IS-IS sends only a single hello for Level 1 and Level 2, making the **level** keyword meaningless on point-to-point links. To modify hello parameters for a point-to-point interface, omit the **level** keyword.

Task ID	Task ID	Operations
	isis	read, write

Examples	The following example shows how to configure a password with HMAC-MD5 authentication for hello packets running on Packet-over-SONET (POS) 0/2/0/3 interface: <pre>RP/0/RP0/CPU0:router(config)# router isis isp RP/0/RP0/CPU0:router(config-isis)# interface POS0/2/0/3 RP/0/RP0/CPU0:router(config-isis-if)# hello-password hmac-md5 clear mypassword</pre>

Related Commands	Command	Description
	hello-password accept	Configures an additional authentication password for an IS-IS interface.

R3.3 Beta Draft—Cisco Confidential Information

hello-password accept

To configure an additional authentication password for an Intermediate System-to-Intermediate System (IS-IS) interface, use the **hello-password accept** command in router configuration mode. To disable authentication, use the **no** form of this command.

hello-password accept {clear | encrypted} password [level {1 | 2}]

no hello-password accept {clear | encrypted} password

Syntax Description

clear	Specifies that the password be unencrypted.
encrypted	Specifies that the password be encrypted using a two-way algorithm.
<i>password</i>	Authentication password you assign.
level {1 2}	(Optional) Specifies the password for Level 1 or Level 2 independently.

Defaults

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Router configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **hello-password accept** command to add an additional password for an IS-IS interface. An authentication password must be configured using the **hello-password** command before an accept password can be configured for the corresponding level.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure an accept Level 1 IS-IS interface password:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# hello-password accept encrypted password1 level 1
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	hello-password	Configures an authentication password for an IS-IS interface.

R3.3 Beta Draft—Cisco Confidential Information

hostname dynamic disable

To disable Intermediate System-to-Intermediate System (IS-IS) routing protocol dynamic hostname mapping, use the **hostname dynamic** command in router configuration mode. To remove the specified command from the configuration file and restore the system to its default condition, use the **no** form of this command.

hostname dynamic disable

no hostname dynamic disable

Syntax Description	disable	Disables dynamic host naming.

Defaults	Router names are dynamically mapped to system IDs.

Command Modes	Router configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

In an IS-IS routing domain, each router is represented by a 6-byte hexadecimal system ID. When network administrators maintain and troubleshoot networking devices, they must know the router name and corresponding system ID.

Flooding of link-state packets (LSPs) causes the type, length, and value (TLV) object parameters to carry the mapping information across the entire network. Every router in the network, upon receiving the TLV from an LSP, tries to install it in a mapping table. The router then uses the mapping table when it wants to convert a system ID to a router name.

To display the entries in the mapping tables, use the **show isis hostname** command.

Using the **no** form of the command removes the specified command from the configuration file and restores the system to its default condition with respect to the command. We recommend that you use the **disable** keyword rather than the **no** form of the command to disable the functionality of the command. The **no** form of a command is not stored in the configuration file. Instead, the command with the **disable** keyword is stored in the configuration file.

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	isis	read, write

Examples	The following example shows how to disable dynamic mapping of hostnames to system IDs: <pre>RP/0/RP0/CPU0:router(config)# router isis isp RP/0/RP0/CPU0:router(config-isis)# hostname dynamic disable</pre>

Related Commands	Command	Description
	hostname	Specifies the name of the local router.
	show isis hostname	Displays the router name-to-system ID mapping table.

R3.3 Beta Draft—Cisco Confidential Information

ignore-lsp-errors

To override the default setting of a router to ignore Intermediate System-to-Intermediate System (IS-IS) link-state packets (LSPs) that are received with internal checksum errors, use the **ignore-lsp-errors disable** command in router configuration mode. To enable ignoring IS-IS LSP errors, use the **no** form of this command.

ignore-lsp-errors disable

no ignore-lsp-errors

Syntax Description	disable	Disables the functionality of the command.

Defaults	The system purges corrupt LSPs that cause the initiator to regenerate LSPs.

Command Modes	Router configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

The IS-IS protocol definition requires that a received LSP with an incorrect data-link checksum be purged by the receiver, which causes the initiator of the packet to regenerate it. However, if a network has a link that causes data corruption while still delivering LSPs with correct data-link checksums, a continuous cycle of purging and regenerating large numbers of packets can occur. Because this situation could render the network nonfunctional, use this command to ignore these LSPs rather than purge the packets.

The receiving network devices use link-state packets to maintain their routing tables.

Task ID	Task ID	Operations
	isis	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to instruct the router to ignore LSPs that have internal checksum errors:

```
RP/0/RP0/CPU0:router(config)# router isis isp  
RP/0/RP0/CPU0:router(config-isis)# ignore-lsp-errors
```

R3.3 Beta Draft—Cisco Confidential Information

interface (IS-IS)

To configure the Intermediate System-to-Intermediate System (IS-IS) protocol on an interface, use the **interface** command in router configuration mode. To disable IS-IS routing for interfaces, use the **no** form of this command.

interface *type instance*

no interface *type instance*

Syntax Description	<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
	<i>instance</i>	Either a physical interface instance or a virtual interface instance as follows: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults No interfaces are specified.

Command Modes Router configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

An address family must be established on the IS-IS interface before the interface is enabled for IS-IS protocol operation.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to enable an IS-IS multitopology configuration for IPv6 on Packet-over-SONET (POS) interface 0/3/0/0:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# net 49.0000.0000.0001.00
RP/0/RP0/CPU0:router(config-isis)# interface POS0/3/0/0
RP/0/RP0/CPU0:router(config-isis-if)# address-family ipv6 unicast
RP/0/RP0/CPU0:router(config-isis-if-af)# metric-style wide level 1
!
RP/0/RP0/CPU0:router(config)# interface POS0/3/0/0
RP/0/RP0/CPU0:router(config-if)# ipv6 address 2001::1/64
```

Related Commands

Command	Description
log adjacency changes (IS-IS)	Configures the routing level for an instance of the IS-IS routing process.
net	Configures an IS-IS network entity title (NET) for the routing process.
router isis	Enables the IS-IS routing protocol.

R3.3 Beta Draft—Cisco Confidential Information**ispf**

To configure the incremental shortest path first (iSPF) algorithm to calculate network topology, use the **ispf** command in router address family configuration mode. To disable this algorithm function, use the **no** form of this command.

ispf [level {1 | 2}]

no ispf [level {1 | 2}]

Syntax Description	level {1 2}	(Optional) Configures the iSPF algorithm for Level 1 or Level 2 independently.

Defaults	The iSPF algorithm is not configured.

Command Modes	Router address family configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	The startup-delay <i>seconds</i> keyword and argument were removed.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. The iSPF algorithm may be used to reduce the processor load when IS-IS needs to recalculate its topology after minor changes.

Task ID	Task ID	Operations
	isis	read, write

Examples	The following example shows how to configure iSPF for the IPv4 unicast topology at Level 1:

```
RP/0/RP0/CPU0:router(config)# router isis ispf
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# ispf level 1
```

R3.3 Beta Draft – Cisco Confidential Information

is-type

To configure the routing level for an Intermediate System-to-Intermediate System (IS-IS) area, use the **is-type** command in router configuration mode. To set the routing level to the default level, use the **no** form of this command.

is-type {level-1 | level-1-2 | level-2-only}

no is-type

Syntax Description	level-1	Specifies that the router perform only Level 1 (intra-area) routing. This router learns only about destinations inside its area. Level 2 (interarea) routing is performed by the closest Level 1-2 router.
	level-1-2	Specifies that the router perform both Level 1 and Level 2 routing. This router runs two instances of the routing process.
	level-2-only	Specifies that the routing process acts as a Level 2 (interarea) router only. This router is part of the backbone, and does not communicate with Level 1-only routers in its own area.

Defaults Both Level 1 and Level 2 are configured if no level is specified.

Command Modes Router configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When the router is configured with Level 1 routing only, this router learns about destinations only inside its area. Level 2 (interarea) routing is performed by the closest Level 1-2 router.

When the router is configured with Level 2 routing only, this router is part of the backbone, and does not communicate with Level 1 routers in its own area.

When the router is configured with both Level 1 and Level 2 routing, this router runs two instances of the routing process. It has one link-state packet database (LSDB) for destinations inside the area (Level 1 routing) and runs a shortest path first (SPF) calculation to discover the area topology. It also has another LSDB with link-state packets (LSPs) of all other backbone (Level 2) routers, and runs another SPF calculation to discover the topology of the backbone and the existence of all other areas.

R3.3 Beta Draft—Cisco Confidential Information

We highly recommend that you configure the type of an IS-IS routing process to establish the proper level of adjacencies. If there is only one area in the network, there is no need to run both Level 1 and Level 2 routing algorithms.

Task ID	Task ID	Operations
	isis	read, write

Examples

The following example shows how to specify that the router is part of the backbone and that it does not communicate with Level 1-only routers:

```
RP/0/RP0/CPU0:router(config)# router isis isp  
RP/0/RP0/CPU0:router(config-isis)# is-type level-2-only
```

Related Commands	Command	Description
	circuit-type	Configures the type of adjacency.
	show isis neighbors	Displays information about IS-IS neighbors.

R3.3 Beta Draft—Cisco Confidential Information

log adjacency changes (IS-IS)

To cause an IS-IS instance to generate a log message when an Intermediate System-to-Intermediate System (IS-IS) adjacency changes state (up or down), use the **log adjacency changes** command in router configuration mode. To restore the default value, use the **no** form of this command.

log adjacency changes

no log adjacency changes

Syntax Description This command has no arguments or keywords.

Defaults No log messages are generated.

Command Modes Router configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **log adjacency changes** command to monitor IS-IS adjacency state changes; it may be very useful when monitoring large networks. Messages are logged using the system error message facility. Messages are of the forms:

```
%ISIS-4-ADJCHANGE: Adjacency to 0001.0000.0008 (POS0/2/1/0) (L2) Up, new adjacency
%ISIS-4-ADJCHANGE: Adjacency to router-grs8 (POS0/2/1/0) (L1) Down, Holdtime expired
```

Using the **no** form of the command removes the specified command from the configuration file and restores the system to its default condition with respect to the command. We recommend that you use the **disable** keyword rather than the **no** form of the command to disable the functionality of the command.

Task ID	Task ID	Operations
	isis	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure the router to log adjacency changes:

```
RP/0/RP0/CPU0:router(config)# router isis isp  
RP/0/RP0/CPU0:router(config-isis)# log adjacency changes
```

Related Commands

Command	Description
logging	Logs messages to a syslog server host.

R3.3 Beta Draft—Cisco Confidential Information

log pdu drops

To log Intermediate System-to-Intermediate System (IS-IS) protocol data units (PDUs) that are dropped, use the **log pdu drops** command in router configuration mode. To disable this function, use the **no** form of this command.

log pdu drops

no log pdu drops

Syntax Description This command has no arguments or keywords.

Defaults PDU logging is disabled.

Command Modes Router configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **log pdu drops** command to monitor a network when IS-IS PDUs are suspected of being dropped. The reason for the PDU being dropped and current PDU drop statistics are recorded.

The following are examples of PDU messages:

```
%ISIS-4-ERR_IIH_INPUT_Q_OVERFLOW: IIH input queue overflow: 86 total drops; 19 IIH drops,
44 LSP drops, 23 SNP drops
%ISIS-4-ERR_LSP_INPUT_Q_OVERFLOW: LSP input queue overflow: 17 total drops; 9 IIH drops, 3
LSP drops, 5 SNP drops
```

Task ID	Task ID	Operations
	isis	read, write

Examples The following example shows how to enable PDU logging:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# log pdu drops
```

R3.3 Beta Draft—Cisco Confidential Information

lsp-gen-interval

To customize IS-IS throttling of link-state packet (LSP) generation, use the **lsp-gen-interval** command in router configuration mode. To restore the default value, use the **no** form of this command.

lsp-gen-interval {[**initial-wait** *initial* | **secondary-wait** *secondary* | **maximum-wait** *maximum*] ...}[**level** {**1** | **2**}]

no lsp-gen-interval

Syntax Description

initial-wait <i>initial</i>	Specifies the initial LSP generation delay (in milliseconds). Range is 0 to 120000 milliseconds.
secondary-wait <i>secondary</i>	Specifies the hold time between the first and second LSP generation (in milliseconds). Range is 1 to 120000 milliseconds.
maximum-wait <i>maximum</i>	Specifies the maximum interval (in milliseconds) between two consecutive occurrences of an LSP being generated. Range is 1 to 120000 milliseconds.
level { 1 2 }	(Optional) Specifies the LSP time interval for Level 1 or Level 2 independently.

Defaults

initial-wait *initial*: 50 milliseconds
secondary-wait *secondary*: 200 milliseconds
maximum-wait *maximum*: 5000 milliseconds

Command Modes

Router configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	The initial-wait <i>initial</i> , secondary-wait <i>secondary</i> , and maximum-wait <i>maximum</i> keywords and arguments were added.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

During prolonged periods of network instability, repeated recalculation of LSPs can cause increased CPU load on the local router. Further, the flooding of these recalculated LSPs to the other Intermediate Systems in the network causes increased traffic and can result in other routers having to spend more time running route calculations.

Use the **lsp-gen-interval** command to reduce the rate of LSP generation during periods of instability in the network. This command can help to reduce CPU load on the router and to reduce the number of LSP transmissions to its IS-IS neighbors.

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	isis	read, write

Examples	The following example shows how to set the maximum interval between two consecutive occurrences of an LSP to 15 milliseconds and the initial LSP generation delta to 5 milliseconds: <pre>RP/0/RP0/CPU0:router(config)# router isis isp RP/0/RP0/CPU0:router(config-isis)# lsp-gen-interval maximum-wait 15 initial-wait 5</pre>

Related Commands	Command	Description
	retransmit-interval (IS-IS)	Configures the amount of time between retransmission of each IS-IS LSP on a point-to-point link.

R3.3 Beta Draft—Cisco Confidential Information

lsp-interval

To configure the amount of time between each link-state packet (LSP) sent on an Intermediate System-to-Intermediate System (IS-IS) interface, use the **lsp-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

lsp-interval *milliseconds* [**level** { **1** | **2** }]

no lsp-interval

Syntax Description	<i>milliseconds</i>	Time delay (in milliseconds) between successive LSPs.
	level { 1 2 }	(Optional) Configures the LSP time delay for Level 1 or Level 2 independently.

Defaults	<i>milliseconds</i> : 33 milliseconds

Command Modes	Interface configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	isis	read, write

Examples	The following example shows how to cause the system to send LSPs every 100 milliseconds (10 packets per second) on Level 1 and Level 2:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# interface POS0/2/0/1
RP/0/RP0/CPU0:router(config-isis-if)# lsp-interval 100
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	retransmit-interval (IS-IS)	Configures the amount of time between retransmission of each IS-IS LSP on a point-to-point link.

R3.3 Beta Draft—Cisco Confidential Information

lsp-mtu

To set the maximum transmission unit (MTU) size of Intermediate System-to-Intermediate System (IS-IS) link-state packets (LSPs), use the **lsp-mtu** command in router configuration mode. To restore the default, use the **no** form of this command.

lsp-mtu *bytes* [**level** {**1** | **2**}]

no **lsp-mtu**

Syntax Description

<i>bytes</i>	Maximum packet size in bytes. The number of bytes must be less than or equal to the smallest MTU of any link in the network. Range is 128 to 4352 bytes.
level { 1 2 }	(Optional) Specifies routing Level 1 or Level 2 independently.

Defaults

bytes: 1492 bytes
Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Router configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Under normal conditions, the default MTU size should be sufficient. However, if the MTU size of a link is less than 1500 bytes, the LSP MTU size must be lowered accordingly on each router in the network. If this action is not taken, routing becomes unpredictable.

This guideline applies to all Cisco networking devices in a network. If any link in the network has a reduced MTU size, all devices must be changed, not just the devices directly connected to the link.

**Note**

Do not set the **lsp-mtu** command (network layer) to a value greater than the link MTU size that is set with the **mtu** command (physical layer).

To be certain about a link MTU size, use the **show isis interface** command to display the value.

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	isis	read, write

Examples	The following example shows how to set the MTU size to 1300 bytes: <pre>RP/0/RP0/CPU0:router(config)# router isis isp RP/0/RP0/CPU0:router(config-isis)# lsp-mtu 1300</pre>

Related Commands	Command	Description
	mtu	Adjusts the maximum packet size or MTU size.
	show isis interface	Displays information about the IS-IS interface.

R3.3 Beta Draft—Cisco Confidential Information

lsp-password

To configure the link-state packet (LSP) authentication password, use the **lsp-password** command in router configuration mode. To remove the **lsp-password** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

```
lsp-password { hmac-md5 | text } { clear | encrypted } password [level { 1 | 2 }] [send-only] [snp send-only]
```

```
no lsp-password
```

Syntax Description		
hmac-md5		Specifies that the password uses HMAC-MD5 authentication.
text		Specifies that the password uses clear text password authentication.
clear		Specifies that the password be unencrypted.
encrypted		Specifies that the password be encrypted using a two-way algorithm.
<i>password</i>		Authentication password you assign.
level { 1 2 }		(Optional) Specifies the password for Level 1 or Level 2 independently.
send-only		(Optional) Adds passwords to LSP and sequence number protocol (SNP) data units when they are sent. Does not check for authentication in received LSPs or sequence number PDUs (SNPs).
snp send-only		(Optional) Adds passwords to SNP data units when they are sent. Does not check for authentication in received SNPs.

Defaults Both Level 1 and Level 2 are configured if no level is specified.

Command Modes Router configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The hmac-md5 , text , clear , and encrypted keywords replaced the 0 and 7 keywords, the snp validate keyword was removed, and the send-only keyword was added
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft – Cisco Confidential Information

When a **text** password is configured, it is exchanged as clear text. Therefore, the **lsp-password** command provides limited security.

When an **HMAC-MD5** password is configured, the password is never sent over the network and is instead used to calculate a cryptographic checksum to ensure the integrity of the exchanged data.

The recommended password configuration is that both incoming and outgoing SNPs be authenticated.



Note

To disable SNP password checking, the **snp send-only** keywords must be specified in the **lsp-password** command.

To configure an additional password, use the **lsp-password accept** command.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure separate Level 1 and Level 2 LSP and SNP passwords, one with HMAC-MD5 authentication and encryption and one with clear text password authentication and no encryption:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# lsp-password hmac-md5 encrypted password1 level 1
RP/0/RP0/CPU0:router(config-isis)# lsp-password text clear password2 level 2
```

Related Commands

Command	Description
lsp-password accept	Configures an additional LSP password when one LSP password is already configured for a level.

R3.3 Beta Draft—Cisco Confidential Information

lsp-password accept

To configure an additional link-state packet (LSP) authentication password, use the **lsp-password accept** command in router configuration mode. To remove the **lsp-password accept** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

lsp-password accept { **clear** | **encrypted** } *password* [**level** { **1** | **2** }]

no lsp-password accept

Syntax Description

clear	Specifies that the password be unencrypted.
encrypted	Specifies that the password be encrypted using a two-way algorithm.
<i>password</i>	Authentication password you assign.
level { 1 2 }	(Optional) Specifies the password for Level 1 or Level 2 independently.

Defaults

Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Router configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **lsp-password accept** command adds an additional password for use when validating incoming LSPs and sequence number PDUs (SNPs). An LSP password must be configured using the **lsp-password** command before an accept password can be configured for the corresponding level.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure an accept Level 1 LSP and SNP password:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# lsp-password accept encrypted password1 level 1
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	lsp-password	Configures an authentication LSP password.

R3.3 Beta Draft—Cisco Confidential Information

lsp-refresh-interval

To set the time between regeneration of link-state packets (LSPs) that contain different sequence numbers, use the **lsp-refresh-interval** command in router configuration mode. To restore the default refresh interval, use the **no** form of this command.

lsp-refresh-interval *seconds* [**level** {**1** | **2**}]

no **lsp-refresh-interval**

Syntax Description

<i>seconds</i>	Refresh interval (in seconds). Range is 1 to 65535 seconds.
level { 1 2 }	(Optional) Specifies routing Level 1 or Level 2 independently.

Defaults

seconds: 900 seconds (15 minutes)
Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Router configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The refresh interval determines the rate at which the software periodically sends the route topology information that it originates. This behavior is done to keep the information from becoming too old. By default, the refresh interval is 7200 seconds (2 hours).

LSPs must be refreshed periodically before their lifetimes expire. The refresh interval must be less than the LSP lifetime specified with this router command. Reducing the refresh interval reduces the amount of time that undetected link-state database corruption can persist at the cost of increased link utilization. (This event is extremely unlikely, however, because there are other safeguards against corruption.)

Increasing the interval reduces the link utilization caused by the flooding of refreshed packets (although this utilization is very small).

Task ID

Task ID	Operations
isis	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to change the LSP refresh interval to 10,800 seconds (3 hours):

```
RP/0/RP0/CPU0:router(config)# router isis isp  
RP/0/RP0/CPU0:router(config-isis)# lsp-refresh-interval 10800
```

Related Commands

Command	Description
max-lsp-lifetime	Sets the maximum time that LSPs persist without being refreshed.

R3.3 Beta Draft—Cisco Confidential Information

maximum-paths (IS-IS)

To configure the maximum number of parallel routes that an IP routing protocol will install into the routing table, use the **maximum-paths** command in router address family configuration mode. To remove the **maximum-paths** command from the configuration file and restore the system to its default condition with respect to the routing protocol, use the **no** form of this command.

maximum-paths *maximum*

no maximum-paths

Syntax Description	<i>maximum</i>	Maximum number of parallel routes that IS-IS can install in a routing table. Range is 1 to 32 for Cisco CRS-1s and 1 to 16 for Cisco XR 12000 Series Routers.

Defaults	<i>maximum</i> (Cisco CRS-1): 8 routes <i>maximum</i> (Cisco XR 12000 Series Router): 8 routes

Command Modes	Router address family configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	isis	read, write

Examples	The following example shows how to allow a maximum of 16 paths to a destination:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# maximum-paths 16
```

R3.3 Beta Draft—Cisco Confidential Information

maximum-redistributed-prefixes (IS-IS)

To specify an upper limit on the number of external prefixes (subject to summarization) that the Intermediate System-to-Intermediate System (IS-IS) protocol advertises, use the **maximum-redistributed-prefixes** command in router address family mode. To disable this feature, use the **no** form of this command.

maximum-redistributed-prefixes *maximum* [**level** {**1** | **2**}]

no maximum-redistributed-prefixes

Syntax Description

<i>maximum</i>	Maximum number of redistributed prefixes advertised. Range is 1 to 28000.
level { 1 2 }	Specifies the interface whose primary IP address is the identifier of the router.

Defaults

maximum: 10000

Command Modes

Router address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **maximum-redistributed-prefixes** command to prevent a misconfiguration from resulting in redistribution of the Internet. If IS-IS encounters more than the maximum number of prefixes, it sets a bi-state alarm. If the number of to-be-redistributed prefixes drops back to the maximum or lower—either through reconfiguration or a change in the redistribution source—IS-IS clears the alarm.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to specify the number of redistributed prefixes at 5000 for Level 2:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# maximum-redistributed-prefixes 5000 level 2
```

R3.3 Beta Draft—Cisco Confidential Information

max-lsp-lifetime

To set the maximum time that link-state packets (LSPs) persist without being refreshed, use the **max-lsp-lifetime** command in router configuration mode. To restore the default time, use the **no** form of this command.

max-lsp-lifetime *seconds* [**level** { **1** | **2** }]

no max-lsp-lifetime

Syntax Description

<i>seconds</i>	Lifetime (in seconds) of the LSP. Range from 1 to 65535 seconds.
level { 1 2 }	(Optional) Specifies routing Level 1 or Level 2 independently.

Defaults

seconds: 1200 seconds (20 minutes)
Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Router configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You might need to adjust the maximum LSP lifetime if you change the LSP refresh interval with the **lsp-refresh-interval** command. The maximum LSP lifetime must be greater than the LSP refresh interval.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to set the maximum time that the LSP persists to 11,000 seconds (more than 3 hours):

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# max-lsp-lifetime 11000
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	lsp-refresh-interval	Sets the LSP refresh interval.

R3.3 Beta Draft—Cisco Confidential Information

mesh-group (IS-IS)

To optimize link-state packet (LSP) flooding in nonbroadcast multiaccess (NBMA) networks with highly meshed, point-to-point topologies, use the **mesh-group** command in interface configuration mode. To remove a subinterface from a mesh group, use the **no** form of this command.

mesh-group {*number* | **blocked**}

no mesh-group

Syntax Description

<i>number</i>	Number identifying the mesh group of which this interface is a member. Range is 1 to 4294967295.
blocked	Specifies that no LSP flooding takes place on this interface.

Defaults

There is no mesh group configuration (normal LSP flooding).

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The { <i>number</i> blocked } argument and keyword was changed from optional to mandatory.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

LSPs first received on subinterfaces that are not part of a mesh group are flooded to all other subinterfaces in the usual way.

LSPs first received on subinterfaces that are part of a mesh group are flooded to all interfaces except those in the same mesh group. If the **blocked** keyword is configured on a subinterface, then a newly received LSP is not flooded out over that interface.

To minimize the possibility of incomplete flooding, you should allow unrestricted flooding over at least a minimal set of links in the mesh. Selecting the smallest set of logical links that covers all physical paths results in very low flooding, but less robustness. Ideally you should select only enough links to ensure that LSP flooding is not detrimental to scaling performance, but enough links to ensure that under most failure scenarios, no router is logically disconnected from the rest of the network. In other words, blocking flooding on all links permits the best scaling performance, but there is no flooding. Permitting flooding on all links results in very poor scaling performance.

R3.3 Beta Draft—Cisco Confidential Information**Note**

See RFC 2973 for details about the mesh group specification.

Task ID

Task ID	Operations
isis	read, write

Examples

In the following example, six interfaces are configured in three mesh groups. LSPs received are handled as follows:

- LSPs first received by Packet-over-SONET (POS) interface 0/1/0/0 are flooded to all interfaces except POS 0/1/0/1 (which is part of the same mesh group) and POS 0/3/0/0 (which is blocked).
- LSPs first received by POS 0/2/0/1 are flooded to all interfaces except POS 0/2/0/0 (which is part of the same mesh group) and POS 0/3/0/0 (which is blocked).
- LSPs first received by POS 0/3/0/0 are not ignored, but flooded as usual to all interfaces. LSPs received first through POS 0/3/0/1 are flooded to all interfaces, except POS 0/3/0/0 (which is blocked).

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# interface POS0/1/0/0
RP/0/RP0/CPU0:router(config-isis-if)# mesh-group 10
RP/0/RP0/CPU0:router(config-isis-if)# exit
RP/0/RP0/CPU0:router(config-isis)# interface POS0/1/0/1
RP/0/RP0/CPU0:router(config-isis-if)# mesh-group 10
RP/0/RP0/CPU0:router(config-isis-if)# exit
RP/0/RP0/CPU0:router(config-isis)# interface POS0/2/0/0
RP/0/RP0/CPU0:router(config-isis-if)# mesh-group 11
RP/0/RP0/CPU0:router(config-isis-if)# exit
RP/0/RP0/CPU0:router(config-isis)# interface POS0/2/0/1
RP/0/RP0/CPU0:router(config-isis-if)# mesh-group 11
RP/0/RP0/CPU0:router(config-isis-if)# exit
RP/0/RP0/CPU0:router(config-isis)# interface POS0/3/0/1
RP/0/RP0/CPU0:router(config-isis-if)# mesh-group 12
RP/0/RP0/CPU0:router(config-isis-if)# exit
RP/0/RP0/CPU0:router(config-isis)# interface POS0/3/0/0
RP/0/RP0/CPU0:router(config-isis-if)# mesh-group blocked
```

R3.3 Beta Draft—Cisco Confidential Information

metric

To configure the metric for an Intermediate System-to-Intermediate System (IS-IS) interface, use the **metric** command in interface address family configuration mode. To restore the default metric value, use the **no metric** form of this command.

metric { *default-metric* | **maximum** } [level { **1** | **2** }]

no metric [level { **1** | **2** }]

Syntax Description

<i>default-metric</i>	Metric assigned to the link and used to calculate the cost from each other router using the links in the network to other destinations. Range is 1 to 63 for narrow metric and 1 to 16777214 for wide metric.
maximum	Specifies maximum wide metric. All routers exclude this link from their shortest path first (SPF).
level { 1 2 }	(Optional) Specifies the SPF calculation for Level 1 or Level 2 independently.

Defaults

default-metric: Default is 10.
Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Interface address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Specifying the **level** keyword resets the metric only for Level 1 or Level 2 routing, respectively.

We highly recommend that you configure metrics on all interfaces.

Metrics of more than 63 cannot be used with narrow metric style.

Task ID

Task ID	Operations
isis	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure Packet-over-SONET 0/1/0/1 interface with a default link-state metric cost of 15 for Level 1:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# interface POS0/1/0/1
RP/0/RP0/CPU0:router(config-isis-if)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-if-af)# metric 15 level 1
```

Related Commands

Command	Description
metric-style narrow	Configures a router running IS-IS so that it generates and accepts old-style TLV objects.
metric-style transition	Configures the software to generate and accept both old-style and new-style TLV objects.
metric-style wide	Configures the software to generate and accept only new-style TLV objects.

R3.3 Beta Draft—Cisco Confidential Information

metric-style narrow

To configure the Intermediate System-to-Intermediate System (IS-IS) software to generate and accept old-style type, length, and value (TLV) objects, use the **metric-style narrow** command in router address family configuration mode. To remove the **metric-style narrow** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

metric-style narrow [**transition**] [**level** {**1** | **2**}]

no metric-style narrow

Syntax Description	transition	(Optional) Instructs the router to accept both old-style and new-style TLV objects. It generates only old-style TLV objects.
	level { 1 2 }	(Optional) Specifies routing Level 1 or Level 2 independently.

Defaults	Old-style TLVs are generated. Both Level 1 and Level 2 are configured if no level is specified.

Command Modes	Router address family configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	IS-IS traffic engineering extensions include new-style TLV objects with wider metric fields than old-style TLV objects. By default, the router generates old-style TLV objects only. To perform Multiprotocol Label Switching traffic engineering (MPLS TE), a router must generate new-style TLV objects.

Task ID	Task ID	Operations
	isis	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to configure the router to generate and accept only old-style TLV objects on router Level 1:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# metric-style narrow level 1
```

Related Commands

Command	Description
metric-style transition	Configures a router to generate and accept both old-style and new-style TLV objects.
metric-style wide	Configures a router to generate and accept only new-style TLV objects.

R3.3 Beta Draft—Cisco Confidential Information

metric-style transition

To configure the Intermediate System-to-Intermediate System (IS-IS) software to generate and accept both old-style and new-style type, length, and value (TLV) objects, use the **metric-style transition** command in router address family configuration mode. To remove the **metric-style transition** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

metric-style transition [level {1 | 2}]

no metric-style transition

Syntax Description	transition	(Optional) Instructs the router to accept both old-style and new-style TLV objects. It generates only old-style TLV objects.
	level {1 2}	(Optional) Specifies routing Level 1 or Level 2 independently.

Defaults	New-style TLVs are not generated. Both Level 1 and Level 2 are configured if no level is specified.

Command Modes	Router address family configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	IS-IS traffic engineering extensions include new-style TLV objects with wider metric fields than old-style TLV objects. By default, the router generates old-style TLV objects only. To perform Multiprotocol Label Switching traffic engineering (MPLS TE), a router needs to generate new-style TLV objects.

Task ID	Task ID	Operations
	isis	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to configure the router to generate and accept both old-style and new-style TLV objects on Level 2:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# metric-style transition level 2
```

Related Commands

Command	Description
metric-style narrow	Configures a router to generate and accept only old-style TLV objects.
metric-style wide	Configures a router to generate and accept only new-style TLV objects.

R3.3 Beta Draft—Cisco Confidential Information

metric-style wide

To configure the Intermediate System-to-Intermediate System (IS-IS) software to generate and accept only new-style type, length, and value (TLV) objects, use the **metric-style wide** command in router address family configuration mode. To remove the **metric-style wide** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

metric-style wide [**transition**] [**level** {**1** | **2**}]

no metric-style wide

Syntax Description	transition	(Optional) Instructs the router to accept both old-style and new-style TLV objects. It generates only old-style TLV objects.
	level { 1 2 }	(Optional) Specifies routing Level 1 or Level 2 independently.

Defaults	Old-style TLV lengths are generated, if this command is not configured. Both Level 1 and Level 2 are configured if no level is specified.

Command Modes	Router address family configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

IS-IS traffic engineering extensions include new-style TLV objects with wider metric fields than old-style TLV objects. If you enter the **metric-style wide** command, a router generates and accepts only new-style TLV objects. Therefore, the router uses less memory and fewer other resources rather than generating both old-style and new-style TLV objects.

To perform MPLS traffic engineering, a router needs to generate new-style TLV objects.

**Note**

This discussion of metric styles and transition strategies is oriented toward traffic engineering deployment. Other commands and models may be appropriate if the new-style TLV objects are desired for other reasons. For example, a network may require wider metrics, but may not use traffic engineering.

metric-style wide

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	isis	read, write

Examples	The following example shows how to configure a router to generate and accept only new-style TLV objects on Level 1: <pre>RP/0/RP0/CPU0:router(config)# router isis isp RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast RP/0/RP0/CPU0:router(config-isis-af)# metric-style wide level 1</pre>

Related Commands	Command	Description
	metric-style narrow	Configures a router to generate and accept only old-style TLV objects.

R3.3 Beta Draft—Cisco Confidential Information

mpls ldp sync

To configure Label Distribution Protocol (LDP) IS-IS synchronization, use the **mpls ldp sync** command in interface address family configuration mode. To disable LDP synchronization, use the **no** form of this command.

mpls ldp sync [level {1 | 2}]

no mpls ldp sync [level {1 | 2}]

Syntax Description	level {1 2}	(Optional) Sets LDP synchronization for the specified level.

Defaults	If a level is not specified, LDP synchronization is set for both levels.

Command Modes	Interface address family configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

MPLS VPN traffic forwarded using LDP labels may be dropped in the following instances:

- A new link is introduced in the network and IS-IS has converged before LDP establishes labels.
- An existing LDP session goes down while IS-IS adjacency is intact over the link.

In both instances, outbound LDP labels are not available for forwarding MPLS traffic. LDP IS-IS synchronization addresses the traffic drop. When the **mpls ldp sync** command is configured, IS-IS advertises the maximum possible link metric until LDP has converged over the link. The link is less preferred and least used in forwarding MPLS traffic. When LDP establishes the session and exchanges labels, IS-IS advertises the regular metric over the link.

**Note**

IS-IS advertises the maximum metric -1 (16777214) if wide metrics are configured since the maximum wide metric is specifically used for link exclusion from the shortest path first algorithm (SPF) (RFC 3784). However, the maximum narrow metric is unaffected by this definition.

Task ID	Task ID	Operations
	isis	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to enable LDP IS-IS synchronization:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# interface POS 0/3/0/0
RP/0/RP0/CPU0:router(config-isis-if)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-if-af)# mpls ldp sync
```

Related Commands

Command	Description
show isis interface	Displays information about the IS-IS interfaces

R3.3 Beta Draft—Cisco Confidential Information

mpls traffic-eng

To configure a router running the Intermediate System-to-Intermediate System (IS-IS) protocol to flood Multiprotocol Label Switching traffic engineering (MPLS TE) link information into the indicated IS-IS level, use the **mpls traffic-eng** command in router address family configuration mode. To disable this feature, use the **no** form of this command.

mpls traffic-eng level { 1 | 2 }

no mpls traffic-eng

Syntax Description	level { 1 2 }	Specifies routing Level 1 or Level 2 independently.

Defaults	Flooding is disabled.

Command Modes	Router address family configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The level keyword became mandatory.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **mpls traffic-eng** command, which is part of the routing protocol tree, to flood link resource information (such as available bandwidth) for appropriately configured links in the link-state packet (LSP) of the router.

Task ID	Task ID	Operations
	isis	read, write

Examples	The following example shows how to turn on MPLS traffic engineering for IS-IS level 1:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# mpls traffic-eng level 1
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	<i>mpls traffic-eng router-id (IS-IS)</i>	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.

R3.3 Beta Draft—Cisco Confidential Information

mpls traffic-eng router-id (IS-IS)

To specify that the Multiprotocol Label Switching traffic engineering (MPLS TE) router identifier for the node is the IP address associated with a given Intermediate System-to-Intermediate System (IS-IS) interface, use the **mpls traffic-eng router-id** command in router address family configuration mode. To disable this feature, use the **no** form of this command.

mpls traffic-eng router-id {*ip-address* | *interface-type interface-instance*}

no mpls traffic-eng router-id

Syntax Description	
<i>ip-address</i>	IP address in four-part, dotted-decimal notation.
<i>interface-type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	Either a physical interface instance or a virtual interface instance as follows: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults Global router identifier is used.

Command Modes Router address family configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The identifier of the router acts as a stable IP address for the traffic engineering configuration. This IP address is flooded to all nodes. For all traffic engineering tunnels originating at other nodes and ending at this node, you must set the tunnel destination to the traffic engineering router of the destination node, because that is the address used by the traffic engineering topology database at the tunnel head for its path calculation.



Note

We recommend that loopback interfaces be used for MPLS TE, because they are more stable than physical interfaces.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to specify the traffic engineering router identifier as the IP address associated with loopback interface 0:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# mpls traffic-eng router-id Loopback0
```

Related Commands

Command	Description
mpls traffic-eng	Turns on flooding of MPLS traffic engineering link information in the indicated IGP level or area.

R3.3 Beta Draft—Cisco Confidential Information

net

To configure an Intermediate System-to-Intermediate System (IS-IS) network entity title (NET) for the routing process, use the **net** command in router configuration mode. To remove the **net** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

net *network-entity-title*

no net

Syntax Description

<i>network-entity-title</i>	NET that specifies the area address and the system ID for an IS-IS routing process.

Defaults

No NET is configured. The IS-IS instance is not operational, because a NET is mandatory.

Command Modes

Router configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Under most circumstances, one and only one NET should be configured.

A NET is a network service access point (NSAP) where the last byte is always zero. On a Cisco router running IS-IS, a NET can be 8 to 20 bytes in length. The last byte is always the n-selector and must be zero. The n-selector indicates to which transport entity the packet is sent. An n-selector of zero indicates no transport entity and means that the packet is for the routing software of the system.

The six bytes directly preceding the n-selector are the system ID. The system ID length is a fixed size and cannot be changed. The system ID must be unique throughout each area (Level 1) and throughout the backbone (Level 2).

All bytes preceding the system ID are the area ID.

A maximum of three NETs for each router is allowed. In rare circumstances, it is possible to configure two or three NETs. In such a case, the area this router is in has three area addresses. Only one area still exists, but it has more area addresses.

Configuring multiple NETs can be temporarily useful in network reconfiguration in which multiple areas are merged, or in which one area is split into more areas. Multiple area addresses enable you to renumber an area individually as needed.

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	isis	read, write

Examples	The following example shows how to configure a router with NET area ID 47.0004.004d.0001 and system ID 0001.0c11.1110: <pre>RP/0/RP0/CPU0:router(config)# router isis isp RP/0/RP0/CPU0:router(config-isis)# net 47.0004.004d.0001.0001.0c11.1110.00</pre>

Related Commands	Command	Description
	log adjacency changes (IS-IS)	Configures the routing level for an instance of the IS-IS routing process.
	router isis	Enables the IS-IS routing protocol and specifies an IS-IS instance.

R3.3 Beta Draft—Cisco Confidential Information

nsf (IS-IS)

To enable nonstop forwarding (NSF) on the next restart, use the **nsf** command in router configuration mode. To restore the default setting, use the **no** form of this command.

nsf {cisco | ietf}

no nsf {cisco | ietf}

Syntax Description

cisco	Specifies Cisco proprietary NSF restart.
ietf	Specifies Internet Engineering Task Force (IETF) NSF restart.

Defaults

NSF is disabled.

Command Modes

Router configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

NSF allows an Intermediate System-to-Intermediate System (IS-IS) instance to restart using checkpointed adjacency and link-state packet (LSP) information, and to perform restart with no impact on its neighbor routers. In other words, there is no impact on other routers in the network due to the destruction and recreation of adjacencies and the system LSP.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to enable Cisco proprietary NSF:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# nsf cisco
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	nsf interface-expires	Configures the number of resends of an acknowledged NSF-restart acknowledgment.
	nsf interface-timer	Configures the time interval after which an unacknowledged IETF NSF restart attempt is repeated.
	nsf lifetime (IS-IS)	Configures the maximum route lifetime following an NSF restart.

R3.3 Beta Draft – Cisco Confidential Information

nsf interface-expires

To configure the number of resends of an acknowledged nonstop forwarding (NSF)-restart acknowledgment, use the **nsf interface-expires** command in router configuration mode. To restore the default value, use the **no** form of this command.

nsf interface-expires *number*

no nsf interface-expires

Syntax Description

<i>number</i>	Number of resends. Range is 1 to 3.

Defaults

number: 3 resends

Command Modes

Router configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When a hello packet sent with the NSF restart flag set is not acknowledged, it is re-sent. Use the **nsf interface-expires** command to control the number of times the NSF hello is re-sent. When this limit is reached on an interface, any neighbor previously known on that interface is assumed to be down and the initial shortest path first (SPF) calculation is permitted, provided that all other necessary conditions are met.

The total time period available for adjacency reestablishment (interface-timer * interface-expires) should be greater than the expected total NSF restart time.

The **nsf interface-expires** command applies only to Internet Engineering Task Force (IETF)-style NSF. It has no effect if Cisco proprietary NSF is configured.

Task ID

Task ID	Operations
isis	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to allow only one retry attempt on each interface if an IETF NSF restart signal is not acknowledged:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# nsf ietf
RP/0/RP0/CPU0:router(config-isis)# nsf interface-expires 1
```

Related Commands

Command	Description
hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the router should declare the adjacency as down.
nsf interface-timer	Configures the time interval after which an unacknowledged IETF NSF restart attempt is repeated.

R3.3 Beta Draft—Cisco Confidential Information

nsf interface-timer

To configure the time interval after which an unacknowledged Internet Engineering Task Force (IETF) nonstop forwarding (NSF) restart attempt is repeated, use the **nsf interface-timer** command in router configuration mode. To restore the default value, use the **no** form of this command.

nsf interface-timer *seconds*

no nsf interface-timer

Syntax Description	<i>seconds</i>	NSF restart time interval (in seconds). Range is 3 to 20 seconds.

Defaults	<i>seconds</i> : 10 seconds

Command Modes	Router configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

When the IETF NSF restart process begins, hello packets send an NSF restart flag that must be acknowledged by the neighbors of the router. Use the **nsf interface-timer** command to control the restart time interval after the hello packet is re-sent. The restart time interval need not match the hello interval.

The **nsf interface-timer** command applies only to IETF-style NSF. It has no effect if Cisco proprietary NSF is configured.

Task ID	Task ID	Operations
	isis	read, write

Examples	The following example shows how to ensure that a hello packet with the NSF restart flag set is sent again every 5 seconds until the flag is acknowledged:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# nsf ietf
RP/0/RP0/CPU0:router(config-isis)# nsf interface-timer 5
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	nsf interface-expires	Configures the number of resends of an acknowledged NSF-restart acknowledgment.
	hello-interval (IS-IS)	Specifies the length of time between hello packets that the software sends.

R3.3 Beta Draft—Cisco Confidential Information

nsf lifetime (IS-IS)

To configure the maximum route lifetime following a nonstop forwarding (NSF) restart, use the **nsf lifetime** command in router configuration mode. To restore the default value, use the **no** form of this command.

nsf lifetime *seconds*

no nsf lifetime

Syntax Description	<i>seconds</i>	Maximum route lifetime (in seconds) following an NSF restart. Range is 5 to 300 seconds.

Defaults	<i>seconds</i> : 60 seconds (1 minute)

Command Modes	Router configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **nsf lifetime** command to set the maximum available time for the reacquisition of checkpointed adjacencies and link-state packets (LSPs) during a Cisco proprietary NSF restart. LSPs and adjacencies not recovered during this time period are abandoned, thus causing changes to the network topology.

The **nsf lifetime** command applies only to Cisco proprietary NSF. It has no effect if Internet Engineering Task Force (IETF)-style NSF is configured.

Task ID	Task ID	Operations
	isis	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure the router to allow only 20 seconds for the entire NSF process:

```
RP/0/RP0/CPU0:router(config)# router isis isp  
RP/0/RP0/CPU0:router(config-isis)# nsf cisco  
RP/0/RP0/CPU0:router(config-isis)# nsf lifetime 20
```

R3.3 Beta Draft—Cisco Confidential Information

passive (IS-IS)

To suppress Intermediate System-to-Intermediate System (IS-IS) packets from going to the interface, use the **passive** command in interface configuration mode. To restore IS-IS packets coming to an interface, use the **no** form of this command.

passive

no passive

Syntax Description This command has no arguments or keywords.

Defaults Interface is active.

Command Modes Interface configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	isis	read, write

Examples The following example shows how to configure the router to suppress IS-IS packets on Packet-over-SONET (POS) interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# interface POS0/1/0/1
RP/0/RP0/CPU0:router(config-isis-if)# passive
```

Related Commands	Command	Description
	suppressed	Allows the IS-IS interface to participate in forming adjacencies without advertising connected prefixes in the LSPs.

R3.3 Beta Draft—Cisco Confidential Information

point-to-point

To configure a network of only two networking devices that use broadcast media and the integrated Intermediate System-to-Intermediate System (IS-IS) routing protocol to function as a point-to-point link instead of a broadcast link, use the **point-to-point** command in interface configuration mode. To disable the point-to-point usage, use the **no** form of this command.

point-to-point

no point-to-point

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Interface configuration

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **point-to-point** command only on broadcast media in a network with two networking devices. The command causes the system to issue packets point-to-point rather than as broadcasts. Configure the command on both networking devices in the network.

Task ID	Task ID	Operations
	isis	read, write

Examples The following example shows how to configure a 10-Gb Ethernet interface to act as a point-to-point interface:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# interface TenGigE 0/6/0/0
RP/0/RP0/CPU0:router(config-isis-if)# point-to-point
```


R3.3 Beta Draft – Cisco Confidential Information

priority (IS-IS)

To configure the priority of designated routers, use the **priority** command in interface configuration mode. To reset the default priority, use the **no** form of this command.

priority *value* [**level** {**1** | **2**}]

no priority *value*

Syntax Description

<i>value</i>	Priority of a router. Range is 0 to 127.
level { 1 2 }	(Optional) Specifies routing Level 1 or Level 2 independently.

Defaults

value: 64
Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Priorities can be configured for Level 1 and Level 2 independently. Specifying Level 1 or Level 2 resets priority only for Level 1 or Level 2 routing, respectively. Specifying no level allows you to configure all levels.

The priority is used to determine which router on a LAN is the designated router or Designated Intermediate System (DIS). The priorities are advertised in the hello packets. The router with the highest priority becomes the DIS.

In the Intermediate System-to-Intermediate System (IS-IS) protocol, there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a router with a higher priority comes online, it takes over the role from the current DIS. For equal priorities, the higher MAC address breaks the tie.

Task ID

Task ID	Operations
isis	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to give Level 1 routing priority by setting the priority level to 80. This router is now more likely to become the DIS.

```
RP/0/RP0/CPU0:router(config)# router isis isp  
RP/0/RP0/CPU0:router(config-isis)# interface TenGigE0/6/0/0  
RP/0/RP0/CPU0:router(config-isis-if)# priority 80 level 1
```

R3.3 Beta Draft—Cisco Confidential Information

propagate level

To propagate routes from one Intermediate System-to-Intermediate System (IS-IS) level into another level, use the **propagate level** command in router address family configuration mode. To disable propagation, use the **no** form of this command.

propagate level { 1 | 2 } **into level** { 1 | 2 } **distribute-list** *access-list-name*

no propagate

Syntax Description

level { 1 2 }	Propagates from routing Level 1 or Level 2 routes.
into	Propagates from Level 1 or Level 2 routes into Level 1 or Level 2 routes.
distribute-list <i>access-list-name</i>	Specifies certain routes intended by the administrator to be passed from one level into another level. Name or number of the access list controlling packet propagation.

Defaults

Route leaking is disabled.

Command Modes

Router address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

In general, route propagation from Level 1 to Level 2 is automatic. You might want to use this command to better control which Level 1 routes can be propagated into Level 2.

Propagating Level 2 routes into Level 1 is called *route leaking*. Route leaking is disabled by default. That is, Level 2 routes are not automatically included in Level 1 link-state packets (LSPs). If you want to leak Level 2 routes into Level 1, you must enable that behavior by using this command.

Propagation from Level 1 into Level 1 and from Level 2 into Level 2 is not allowed.

Task ID

Task ID	Operations
isis	read, write

■ propagate level

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to redistribute Level 2 routes to Level 1:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list 101 permit ip 10.0.0.0 255.0.0.0 10.1.0.1 0.255.255.255
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# net 49.1234.2222.2222.2222.00
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# propagate level 2 into level 1 distribute-list 101
```

Related Commands

Command	Description
redistribute (IS-IS)	Redistributes routes from one IS-IS instance into another process.

R3.3 Beta Draft—Cisco Confidential Information

redistribute (IS-IS)

To redistribute routes from one routing protocol into Intermediate System-to-Intermediate System (IS-IS), use the **redistribute** command in router address family configuration mode. To remove the **redistribute** command from the configuration file and restore the system to its default condition in which the software does not redistribute routes, use the **no** form of this command.

Border Gateway Protocol (BGP)

```
redistribute bgp process-id [level-1 | level-2 | level-1-2] [metric metric-value] [metric-type {internal | external}] [route-policy route-policy-name]
```

```
no redistribute bgp process-id [level-1 | level-2 | level-1-2] [metric metric-value] [metric-type {internal | external}] [route-policy route-policy-name]
```

Connected Routes

```
redistribute connected [level-1 | level-2 | level-1-2] [metric metric-value] [metric-type {internal | external}] [route-policy route-policy-name]
```

```
no redistribute connected [level-1 | level-2 | level-1-2] [metric metric-value] [metric-type {internal | external}] [route-policy route-policy-name]
```

Intermediate System-to-Intermediate System (IS-IS)

```
redistribute isis process-id [level-1 | level-2 | level-1-2] [metric metric-value] [metric-type {internal | external}] [route-policy route-policy-name]
```

```
no redistribute isis process-id [level-1 | level-2 | level-1-2] [metric metric-value] [metric-type {internal | external}] [route-policy route-policy-name]
```

Open Shortest Path First (OSPF)

```
redistribute ospf process-id [level-1 | level-2 | level-1-2] [match {external [1 | 2] | internal | nssa-external [1 | 2]}] [metric metric-value] [metric-type {internal | external}] [route-policy route-policy-name]
```

```
no redistribute ospf process-id [level-1 | level-2 | level-1-2] [match {external [1 | 2] | internal | nssa-external [1 | 2]}] [metric metric-value] [metric-type {internal | external}] [route-policy route-policy-name]
```

Static

```
redistribute static [metric metric-value] [metric-type {1 | 2}] [route-policy route-policy-name] [tag tag-value]
```

```
no redistribute static [metric metric-value] [metric-type {1 | 2}] [route-policy route-policy-name] [tag tag-value]
```

R3.3 Beta Draft—Cisco Confidential Information

Syntax Description		
	<i>process-id</i>	For the bgp keyword, an autonomous system number, which is a 16-bit decimal number. Range is 1 to 65535. For the isis keyword, an IS-IS instance identifier from which routes are to be redistributed. For the ospf keyword, an OSPF process name from which routes are to be redistributed. The value takes the form of a string. A decimal number can be entered, but it is stored internally as a string.
	level-1	(Optional) Specifies that redistributed routes are advertised in the Level-1 LSP of the router.
	level-1-2	(Optional) Specifies that redistributed routes are advertised in the Level-1-2 LSP of the router.
	level-2	(Optional) Specifies that redistributed routes are advertised in the Level-2 LSP of the router.
	metric <i>metric-value</i>	(Optional) Specifies the metric used for the redistributed route. Range is 0 to 16777215. The <i>metric-value</i> must be consistent with the IS-IS metric style of the area and topology into which the routes are being redistributed.
	metric-type { internal external }	(Optional) Specifies the external link type associated with the route advertised into the ISIS routing domain. It can be one of two values: • internal • external Any route with an internal metric (however large the metric is) is preferred over a route with external metric (however small the metric is).
	route-policy <i>route-policy-name</i>	(Optional) Specifies the identifier of a configured policy. A policy is used to filter the importation of routes from this source routing protocol to IS-IS.
	match { internal external [1 2] nssa-external [1 2] }	(Optional) Specifies the criteria by which OSPF routes are redistributed into other routing domains. It can be one or more of the following: • internal—Routes that are internal to a specific autonomous system (intra- and interarea OSPF routes). • external [1 2]—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 external routes. • nssa-external [1 2]—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 not-so-stubby area (NSSA) external routes. For the external and nssa-external options, if a type is not specified, then both Type 1 and Type 2 are assumed.
Defaults	Level 2 is configured if no level is specified. metric-type: internal match: If no match keyword is specified, all OPSF routes are redistributed.	

R3.3 Beta Draft – Cisco Confidential Information

Command Modes Router address family configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	The policy <i>policy-name</i> keyword and argument were changed to route-policy <i>route-policy-name</i> .

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **redistribute** command to control the redistribution of routes between separate IS-IS instances. To control the propagation of routes between the levels of a single IS-IS instance, use the **propagate level** command.

Task ID	Task ID	Operations
	isis	read, write

Examples In this example, IS-IS instance isp_A readadvertises all of the routes of IS-IS instance isp_B in Level 2 LSP. Note that the **level-2** keyword affects which levels instance isp_A advertises the routes in and has no impact on which routes from instance isp_B are advertised (any Level 1 routes from IS-IS instance isp_A are included in the redistribution.)

```
RP/0/RP0/CPU0:router(config)# router isis isp_A
RP/0/RP0/CPU0:router(config-isis)# net 49.1234.2222.2222.00
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# redistribute isis isp level-2
!
RP/0/RP0/CPU0:router(config)# router isis isp_B
RP/0/RP0/CPU0:router(config-isis)# is-type level 1
RP/0/RP0/CPU0:router(config-isis)# net 49.4567.2222.2222.00
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# set-attached-bit
```

Related Commands	Command	Description
	propagate level	Propagates routes from one IS-IS level into another level.

R3.3 Beta Draft—Cisco Confidential Information

retransmit-interval (IS-IS)

To configure the amount of time between retransmission of each Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP) on a point-to-point link, use the **retransmit-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

retransmit-interval *seconds* [**level** {**1** | **2**}]

no retransmit-interval

Syntax Description

<i>seconds</i>	Time (in seconds) between retransmission of each LSP. It is an integer that should be greater than the expected round-trip delay between any two networking devices on the attached network. Range is 0 to 65535 seconds.
level { 1 2 }	(Optional) Specifies routing Level 1 or Level 2 independently.

Defaults

seconds: 5 seconds

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The level { 1 2 } keywords were added.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

To prevent needless transmission results, the *seconds* argument should be conservative.

The **retransmit-interval** command has no effect on LAN (multipoint) interfaces. On point-to-point links, the value can be increased to enhance network stability.

Because retransmissions occur only when LSPs are dropped, setting this command to a higher value has little effect on reconvergence. The more neighbors networking devices have, and the more paths over which LSPs can be flooded, the higher this value can be made.

Task ID

Task ID	Operations
isis	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure Packet-over-SONET (POS) interface 0/2/0/1 for retransmission of IS-IS LSPs every 60 seconds for a large serial line:

```
RP/0/RP0/CPU0:router(config)# router isis isp  
RP/0/RP0/CPU0:router(config-isis)# interface POS0/2/0/1  
RP/0/RP0/CPU0:router(config-isis-if)# retransmit-interval 60
```

Related Commands

Command	Description
retransmit-throttle-interval	Configures the amount of time between retransmissions of any IS-IS LSPs on a point-to-point interface.

R3.3 Beta Draft—Cisco Confidential Information

retransmit-throttle-interval

To configure the amount of time between retransmissions on each Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP) on a point-to-point interface, use the **retransmit-throttle-interval** command in interface configuration mode. To remove the command from the configuration file and restore the system to its default condition, use the **no** form of this command.

retransmit-throttle-interval *milliseconds* [**level** {**1** | **2**}]

no retransmit-throttle-interval

Syntax Description

<i>milliseconds</i>	Minimum delay (in milliseconds) between LSP retransmissions on the interface. Range is 0 to 65535.
level { 1 2 }	(Optional) Specifies routing Level 1 or Level 2 independently.

Defaults

Default is 0.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The level { 1 2 } keywords were added.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **retransmit-throttle-interval** command to define the minimum period of time that must elapse between retransmitting any two LSPs on an interface. The **retransmit-throttle-interval** command may be useful in very large networks with many LSPs and many interfaces as a way of controlling LSP retransmission traffic. This command controls the rate at which LSPs can be re-sent on the interface.

Task ID

Task ID	Operations
isis	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to configure Packet-over-SONET (POS) interface 0/2/0/1 to limit the rate of LSP retransmissions to one every 300 milliseconds:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# interface POS0/2/0/1
RP/0/RP0/CPU0:router(config-isis-if)# retransmit-throttle-interval 300
```

Related Commands

Command	Description
lsp-gen-interval	Configures the minimum interval time between regenerating the same LSP.
retransmit-interval (IS-IS)	Configures the amount of time between retransmission of each IS-IS LSP over a point-to-point link.

R3.3 Beta Draft—Cisco Confidential Information

router isis

To enable the Intermediate System-to-Intermediate System (IS-IS) routing protocol and to specify an IS-IS instance, use the **router isis** command in global configuration mode. To disable IS-IS routing, use the **no** form of this command.

router isis *instance-id*

no router isis *instance-id*

Syntax Description

instance-id Name of the routing process.

Defaults

An IS-IS routing protocol is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **router isis** command to create an IS-IS routing process. An appropriate network entity title (NET) must be configured to specify the address of the area (Level 1) and system ID of the router. Routing must be enabled on one or more interfaces before adjacencies may be established and dynamic routing is possible.

Task ID

Task ID	Operations
isis	read, write

Examples

The following example shows how to configure IS-IS for IP routing:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# net 49.0001.0000.0001.00
```

R3.3 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	net	Configures an IS-IS NET for the routing process.

R3.3 Beta Draft—Cisco Confidential Information

set-attached-bit

To configure an Intermediate System-to-Intermediate System (IS-IS) instance with an attached bit in the Level 1 link-state packet (LSP), use the **set-attached-bit** command in router address family configuration mode. To remove the **set-attached-bit** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

set-attached-bit

no set-attached-bit

Syntax Description

This command has no arguments or keywords.

Defaults

Attached bit is not set in the LSP.

Command Modes

Router address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **set-attached bit** command to set an IS-IS instance with an attached bit in the Level 1 LSP that allows another IS-IS instance to redistribute Level 2 topology. The attached bit is used when the Level 2 connectivity from another IS-IS instance is advertised by the Level 1 attached bit.

Cisco IOS XR software does not support multiple Level 1 areas in a single IS-IS routing instance. But the equivalent functionality is achieved by redistribution of routes between two IS-IS instances by using the **redistribute (IS-IS)** command.

The attached bit is configured for a specific address family only if the **single-topology** command is not configured.



Note

If connectivity for the Level 2 instance is lost, the attached bit in the Level 1 instance LSP continues sending traffic to the Level 2 instance and causes the traffic to be dropped.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	isis	read, write

Examples

The following example shows how to set the attached bit for a Level 1 instance that allows the Level 2 instance to redistribute routes from the Level 1 instance:

```
RP/0/RP0/CPU0:router(config)# router isis 1
RP/0/RP0/CPU0:router(config-isis)# net 49.0001.0001.0001.0001.00
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# redistribute isis 2 level 2
!
RP/0/RP0/CPU0:router(config-isis-af)# interface POS0/3/0/0
RP/0/RP0/CPU0:router(config-isis-af-if)# address-family ipv4 unicast
!
!
RP/0/RP0/CPU0:router(config)# router isis 2
RP/0/RP0/CPU0:router(config-isis)# is-type level-1
RP/0/RP0/CPU0:router(config-isis)# net 49.0002.0001.0001.0002.00
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# set-attached-bit
!
RP/0/RP0/CPU0:router(config-isis-af)# interface POS0/1/0/0
RP/0/RP0/CPU0:router(config-isis-af-if)# address-family ipv4 unicast
```

Related Commands

Command	Description
redistribute (IS-IS)	Redistributes routes from one IS-IS instance into another instance.
single-topology	Configures the link topology for IPv4 when IPv6 is configured.

R3.3 Beta Draft—Cisco Confidential Information

set-overload-bit

To configure the router to signal other routers not to use it as an intermediate hop in their shortest path first (SPF) calculations, use the **set-overload-bit** command in router configuration mode. To remove the designation, use the **no** form of this command.

set-overload-bit [**on-startup** {*delay* | **wait-for-bgp**}] [**level** {**1** | **2**}]

no set-overload-bit

Syntax Description	on-startup	(Optional) Sets the overload bit only temporarily after reboot.
	<i>delay</i>	(Optional) Time (in seconds) to advertise when the router is overloaded after reboot. Range is 5 to 86400 seconds (86400 seconds = 1 day).
	wait-for-bgp	(Optional) Sets the overload bit on startup until the Border Gateway Protocol (BGP) signals converge or time out.
	level { 1 2 }	(Optional) Specifies the overload bit for Level 1 or Level 2 independently.

Defaults

The overload bit is not set.
Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Router configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **set-overload-bit** command to force the router to set the overload bit in its nonpseudonode link-state packets (LSPs). Normally the setting of the overload bit is allowed only when a router experiences problems. For example, when a router is experiencing a memory shortage, the reason might be that the link-state database is not complete, resulting in an incomplete or inaccurate routing table. If the overload bit is set in the LSPs of the unreliable router, other routers can ignore the router in their SPF calculations until it has recovered from its problems. The result is that no paths through the unreliable router are seen by other routers in the Intermediate System-to-Intermediate System (IS-IS) area. However, IP prefixes directly connected to this router are still reachable.

R3.3 Beta Draft—Cisco Confidential Information

The **set-overload-bit** command can be useful when you want to connect a router to an IS-IS network, but do not want real traffic flowing through it under any circumstances.

Routers with overload bit set are:

- A test router in the lab, connected to a production network.

A router configured as an LSP flooding server, for example, on a nonbroadcast multiaccess (NBMA) network, in combination with the mesh group feature.

Task ID	Task ID	Operations
	isis	read, write

Examples

The following example shows how to configure the overload bit:

```
RP/0/RP0/CPU0:router(config)# router isis isp  
RP/0/RP0/CPU0:router(config-isis)# set-overload-bit
```

R3.3 Beta Draft—Cisco Confidential Information

show isis adjacency

To display Intermediate System-to-Intermediate System (IS-IS) adjacencies, use the **show isis adjacency** command in EXEC mode.

```
show isis [instance instance-id] adjacency [level {1 | 2}] [interface-type interface-instance]
[detail] [systemid system-id]
```

Syntax Description		
instance <i>instance-id</i>	(Optional) Displays the IS-IS adjacencies for the specified IS-IS instance only.	The <i>instance-id</i> argument is the instance identifier (alphanumeric) defined by the router isis command.
level {1 2}	(Optional) Displays the IS-IS adjacencies for Level 1 or Level 2 independently.	
<i>interface-type</i>	Interface type. For more information, use the question mark (?) online help function.	
<i>interface-instance</i>	Either a physical interface instance or a virtual interface instance as follows:	- Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
detail	(Optional) Displays neighbor IP addresses and active topologies.	
systemid <i>system-id</i>	(Optional) Displays the information for the specified router only.	

Defaults

No instance ID specified displays IS-IS adjacencies for all the IS-IS instances. Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

EXEC

R3.3 Beta Draft—Cisco Confidential Information

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis adjacency** command:

```
RP/0/RP0/CPU0:router# show isis adjacency
```

```
IS-IS p Level-1 adjacencies:
```

System Id	Interface	SNPA	State	Hold	Changed	NSF	BFD
12a4	PO0/1/0/1	*PtoP*	Up	23	00:00:06	Capable	Init
12a4	Gi0/6/0/2	0004.2893.f2f6	Up	56	00:04:01	Capable	Up

```
Total adjacency count: 2
```

```
IS-IS p Level-2 adjacencies:
```

System Id	Interface	SNPA	State	Hold	Changed	NSF	BFD
12a4	PO0/1/0/1	*PtoP*	Up	23	00:00:06	Capable	None
12a4	Gi0/6/0/2	0004.2893.f2f6	Up	26	00:00:13	Capable	Init

```
Total adjacency count: 2
```

Table 38 describes the significant fields shown in the display.

Table 38 *show isis adjacency Field Descriptions*

Field	Description
Level-1	Level 1 adjacencies.
Level-2	Level 2 adjacencies.
System ID	Dynamic hostname of the system. The hostname is specified using the hostname command. If the dynamic hostname is not known or hostname dynamic disable command has been executed, the 6-octet system ID is used.
Interface	Interface used to reach the neighbor.
SNPA	Data-link address (also known as the Subnetwork Point of Attachment [SNPA]) of the neighbor.
State	State of the neighboring interface.
Holdtime	Hold time of the neighbor.

show isis adjacency

R3.3 Beta Draft – Cisco Confidential Information

Table 38 *show isis adjacency Field Descriptions (continued)*

Field	Description
Changed	Time the neighbor has been up (in hours:minutes:seconds).
NSF	Specifies whether the neighbor can adhere to the IETF-NSF restart mechanism.
BFD	Specifies the Bidirectional Forwarding Detection (BFD) status for the interface.

Related Commands

Command	Description
show isis neighbors	Displays information about IS-IS neighbors.

R3.3 Beta Draft – Cisco Confidential Information

show isis adjacency-log

To display the Intermediate System-to-Intermediate System (IS-IS) adjacency log, use the **show isis adjacency-log** command in EXEC mode.

show isis adjacency-log [*last number* | *first number* | *level {1 | 2}*]

Syntax Description	<i>last number</i>	(Optional) Specifies that the output is restricted to the last <i>number</i> of entries.
	<i>first number</i>	(Optional) Specifies that the output is restricted to the first <i>number</i> of entries.
	<i>level {1 2}</i>	(Optional) Displays the IS-IS adjacency log for Level 1 or Level 2 independently.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	isis	read

Examples	The following is sample output from the show isis adjacency-log command:

```
RP/0/RP0/CPU0:router# show isis adjacency-log
```

```
IS-IS 10 Level 1 Adjacency log
When      System      Interface      State  Details
4d00h     12a1                PO0/5/0/0     d -> i
4d00h     12a1                PO0/5/0/0     i -> u  New adjacency
                                         IPv4 Unicast Up
4d00h     12a1                Gi0/6/0/0     d -> u  New adjacency
4d00h     12a1                Gi0/6/0/0     u -> d  Interface state
```

```
show isis adjacency-log
```

R3.3 Beta Draft – Cisco Confidential Information

```

down
3d17h          12a1          Gi0/6/0/0          d -> u  New adjacency
3d17h          12a1          Gi0/6/0/0          u -> d  Interface state
down
01:44:07      12a1          Gi0/6/0/0          d -> u  New adjacency

IS-IS 10 Level 2 Adjacency log
When          System        Interface        State  Details
4d00h         12a1          PO0/5/0/0       d -> i
4d00h         12a1          PO0/5/0/0       i -> u  New adjacency
                                   IPv4 Unicast Up
4d00h         12a1          Gi0/6/0/0       d -> u  New adjacency
4d00h         12a1          Gi0/6/0/0       u -> d  Interface state
down
3d17h         12a1          Gi0/6/0/0       d -> u  New adjacency
3d17h         12a1          Gi0/6/0/0       u -> d  Interface state
down
01:44:07      12a1          Gi0/6/0/0       d -> u  New adjacency

```

Table 39 describes the significant fields shown in the display.

Table 39 *show isis adjacency-log Field Descriptions*

Field	Description
When	Elapsed time (in hh:mm:ss) since the event was logged.
System	System ID of the adjacent router.
Interface	Specific interface involved in the adjacency change.
State	State transition for the logged event.
Details	Description of the adjacency change.

R3.3 Beta Draft—Cisco Confidential Information

show isis checkpoint adjacency

To display the Intermediate System-to-Intermediate System (IS-IS) checkpoint adjacency database, use the **show isis checkpoint adjacency** command in EXEC mode.

show isis [*instance instance-id*] **checkpoint adjacency**

Syntax Description	instance <i>instance-id</i> (Optional) Displays the IS-IS checkpoint adjacencies for the specified IS-IS instance only. The <i>instance-id</i> argument is the instance identifier (alphanumeric) defined by the router isis command.

Defaults	No instance ID specified displays IS-IS checkpoint adjacencies for all the IS-IS instances.

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the show isis checkpoint adjacency command to display the checkpointed adjacencies. With this information you can restore the adjacency database during a Cisco proprietary nonstop forwarding (NSF) restart. This command, with the show isis adjacency command, may be used to verify the consistency of the two databases.

Task ID	Task ID	Operations
	isis	read

Examples	The following is sample output from the show isis checkpoint adjacency command:

```
RP/0/RP0/CPU0:router# show isis checkpoint adjacency
```

Interface	Level	System ID	State	Circuit ID	Chkpt ID
POS3/0/0/1	1	router-gsr8	Up	0001.0000.0008.04	80011fec
POS0/4/0/1	1	router-gsr9	Up	0001.0000.0006.01	80011fd8
POS3/0/0/1	2	router-gsr8	Up	0001.0000.0008.04	80011fc4

R3.3 Beta Draft – Cisco Confidential Information

Table 40 describes the significant fields shown in the display.

Table 40 *show isis checkpoint adjacency Field Descriptions*

Field	Description
Interface	Interface used to reach the neighbor.
Level	Lists either routers with Level 1 or Level 2 adjacency configured.
System ID	Dynamic hostname of the system. The hostname is specified using the hostname command. If the dynamic hostname is not known or hostname dynamic disable command has been executed, the 6-octet system ID is used.
State	State of the neighboring interface.
Circuit ID	Unique ID issued to a circuit at its creation.
Chkpt ID	Unique ID issued to the checkpoint at its creation.

Related Commands

Command	Description
show isis adjacency	Displays IS-IS adjacencies.
show isis checkpoint lsp	Displays the IS-IS checkpoint LSP database.

R3.3 Beta Draft—Cisco Confidential Information

show isis checkpoint interface

To display the Intermediate System-to-Intermediate System (IS-IS) checkpoint interfaces, use the **show isis checkpoint interface** command in EXEC mode.

show isis checkpoint interface

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	isis	read

Examples The following is sample output from the **show isis checkpoint interface** command:

```
RP/0/RP0/CPU0:router# show isis checkpoint interface

IS-IS 10 checkpoint interface
Interface      Index  CircNum  DIS Areas  Chkpt ID
PO0/5/0/0      0      0        NONE      80002fe8
Gi0/6/0/0      1      3        L1L2      80002fd0
```

Table 41 describes the significant fields shown in the display.

R3.3 Beta Draft—Cisco Confidential Information

Table 41 *show isis checkpoint interface Field Descriptions*

Field	Description
Interface	Interface used to reach the neighbor.
Index	Interface index assigned to an interface upon its creation.
CircNum	Unique ID issued to a circuit internally.
DIS Areas	Designated Intermediate System area.
Chkpt ID	Unique ID issued to the checkpoint at its creation.

R3.3 Beta Draft—Cisco Confidential Information

show isis checkpoint lsp

To display the Intermediate System-to-Intermediate System (IS-IS) checkpoint link-state packet (LSP) protocol data unit (PDU) identifier database, use the **show isis checkpoint lsp** command in EXEC mode.

show isis [**instance** *instance-id*] **checkpoint lsp**

Syntax Description	instance <i>instance-id</i> (Optional) Displays the IS-IS checkpoint LSPs for the specified instance only. The <i>instance-id</i> argument is the instance identifier (alphanumeric) defined by the router isis command.

Defaults	No instance ID specified displays IS-IS checkpoint LSPs for all the IS-IS instances.

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	The checkpointed LSPs displayed by this command are used to restore the LSP database during a Cisco proprietary nonstop forwarding (NSF) restart. The show isis checkpoint lsp command, with the show isis database command, may be used to verify the consistency of the two databases.

Task ID	Task ID	Operations
	isis	read

Examples	The following is sample output from the show isis checkpoint lsp command:

```
RP/0/RP0/CPU0:router# show isis checkpoint lsp
```

```
Level  LSPID                Chkpt ID
1      router-gsr6.00-00    80011f9c
1      router-gsr6.01-00    80011f88
1      router-gsr8.00-00    80011f74
1      router-gsr9.00-00    80011f60
```

```
show isis checkpoint lsp
```

R3.3 Beta Draft—Cisco Confidential Information

```
2      router-gsr6.00-00  80011f4c
2      router-gsr6.01-00  80011f38
2      router-gsr8.00-00  80011f24
2      router-gsr9.00-00  80011f10
Total LSP count: 8 (L1: 4, L2 4, local L1: 2, local L2 2)
```

Table 42 describes the significant fields shown in the display.

Table 42 *show isis checkpoint lsp Field Descriptions*

Field	Description
Level	Routers with Level 1 or Level 2 adjacency configured.
LSPID	LSP identifier. The first six octets form the system ID of the router that originated the LSP. The next octet is the pseudonode ID. When this byte is zero, the LSP describes links from the system. When it is nonzero, the LSP is a so-called nonpseudonode LSP. This is similar to a router link-state advertisement (LSA) in the Open Shortest Path First (OSPF) protocol. The LSP describes the state of the originating router. For each LAN, the designated router for that LAN creates and floods a pseudonode LSP, describing all systems attached to that LAN. The last octet is the LSP number. If there is more data than can fit in a single LSP, the LSP is divided into multiple LSP fragments. Each fragment has a different LSP number. An asterisk (*) indicates that the LSP was originated by the system on which this command is issued.
Chkpt ID	Unique ID issued to the checkpoint at its creation.

Related Commands

Command	Description
show isis checkpoint adjacency	Displays the IS-IS checkpoint adjacency database.
show isis database	Displays the IS-IS link-state database.

R3.3 Beta Draft—Cisco Confidential Information

show isis database

To display the Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP) database, use the **show isis database** command in EXEC mode.

show isis [**instance** *instance-id*] **database** [**level** {**1** | **2**}] [**detail** | **summary** | **verbose**] [***** | *lsp-id*]

Syntax Description		
instance <i>instance-id</i>	(Optional) Displays the IS-IS LSP database for the specified instance only.	The <i>instance-id</i> argument is the instance identifier (alphanumeric) defined by the router isis command.
level { 1 2 }	(Optional) Displays the IS-IS LSP database for Level 1 or Level 2 independently.	
detail	(Optional) Displays the contents of each LSP.	
summary	(Optional) Displays the LSP ID number, sequence number, checksum, hold time, and bit information.	
verbose	(Optional) Displays the contents of each LSP.	
* <i>lsp-id</i>	(Optional) LSP protocol data units (PDUs) identifier. Displays the contents of a single LSP by its ID number or may contain an * as a wildcard character.	

Defaults No instance ID specified displays the IS-IS LSP database for all the IS-IS instances. Both Level 1 and Level 2 is configured if no level is specified.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Each of the options for the **show isis database** command can be entered in an arbitrary string within the same command entry. For example, the following are both valid command specifications and provide the same output: **show isis database detail level 2** and **show isis database level 2 detail**.

The **summary** keyword used with this command allows you to filter through a large IS-IS database and quickly identify problematic areas.

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	isis	read

Examples

The following is sample output from the **show isis database** command with no keywords is specified:

```
RP/0/RP0/CPU0:router# show isis database

IS-IS Area a1 (Level-1) Link State Database
LSPID                LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
router-gsr6.00-00    * 0x00000016  0x62c8        896           0/0/0
router-gsr6.01-00    * 0x0000000f  0x56d9        902           0/0/0
router-gsr8.00-00    0x00000019  0x4b6d        1015          0/0/0
router-gsr9.00-00    0x00000016  0x33b7        957           0/0/0
```

Total LSP count: 4 (L1: 4, L2 0, local L1: 2, local L2 0)

Table 43 describes the significant fields shown in the display.

Table 43 show isis database Field Descriptions

Field	Description
LSPID	LSP identifier. The first six octets form the system ID of the router that originated the LSP. The next octet is the pseudonode ID. When this byte is zero, the LSP describes links from the system. When it is nonzero, the LSP is a so-called nonpseudonode LSP. This is similar to a router link-state advertisement (LSA) in the Open Shortest Path First (OSPF) protocol. The LSP describes the state of the originating router. For each LAN, the designated router for that LAN creates and floods a pseudonode LSP, describing all systems attached to that LAN. The last octet is the LSP number. If there is more data than can fit in a single LSP, the LSP is divided into multiple LSP fragments. Each fragment has a different LSP number. An asterisk (*) indicates that the LSP was originated by the system on which this command is issued.
LSP Seq Num	Sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
LSP Checksum	Checksum of the entire LSP packet.

R3.3 Beta Draft—Cisco Confidential Information

Table 43 *show isis database Field Descriptions (continued)*

Field	Description
LSP Holdtime	Time the LSP remains valid (in seconds). An LSP hold time of zero indicates that this LSP was purged and is being removed from the link-state database (LSDB) of all routers. The value indicates how long the purged LSP stays in the LSDB before being completely removed.
ATT/P/OL	ATT—Attach bit. This bit indicates that the router is also a Level 2 router, and it can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers use the Attach bit to find the closest Level 2 router. They point to a default route to the closest Level 2 router. P—P bit. Detects if the intermediate system is area partition repair capable. Cisco and other vendors do not support area partition repair. OL—Overload bit. Determines if the IS is congested. If the Overload bit is set, other routers do not use this system as a transit router when calculating routers. Only packets for destinations directly connected to the overloaded router are sent to this router.

The following is sample out from the **show isis database** command with the **summary** keyword:

RP/0/RP0/CPU0:router# **show isis database summary**

```
IS-IS 10 Database Summary for all LSPs
              Active              Purged              All
              L1   L2   Total    L1   L2   Total    L1   L2   Total
              -----
Fragment 0 Counts
  Router LSPs:    1    1    2        0    0    0        1    1    2
  Pseudo-node LSPs: 0    0    0        0    0    0        0    0    0
  All LSPs:       1    1    2        0    0    0        1    1    2
Per Topology
  IPv4 Unicast
    ATT bit set LSPs: 0    0    0        0    0    0        0    0    0
    OVL bit set LSPs: 0    0    0        0    0    0        0    0    0
All Fragment Counts
  Router LSPs:    1    1    2        0    0    0        1    1    2
  Pseudo-node LSPs: 0    0    0        0    0    0        0    0    0
  All LSPs:       1    1    2        0    0    0        1    1    2
```

Table 44 describes the significant fields shown in the display.

Table 44 *show isis database summary Field Descriptions*

Field	Description
Router LSPs:	Active, purged, and total LSPs associated with routers.
Pseudo-node LSPs:	Active, purged, and total LSPs associated with pseudonodes.
All LSPs:	Total active and purged LSPs.

R3.3 Beta Draft—Cisco Confidential Information

Table 44 *show isis database summary Field Descriptions (continued)*

Field	Description
ATT bit set LSPs	Attach bit (ATT). Indicates that the router is also a Level 2 router, and it can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers use the Attach bit to find the closest Level 2 router. They point to a default route to the closest Level 2 router.
OVL bit set LSPs	Overload bit. Indicates if the IS is congested. If the Overload bit is set, other routers do not use this system as a transit router when calculating routers. Only packets for destinations directly connected to the overloaded router are sent to this router.

The following is sample output from the **show isis database** command with the **detail** keyword specified:

```
RP/0/RP0/CPU0:router# show isis instance isp database detail
```

```
IS-IS isp (Level-1) Link State Database
```

```

LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
router-5.00-00  0x00000003   0x8074460    457           0/0/0
  Area Address: 49
  NLPID:        0xcc
  Hostname:     router-5
  IP Address:   172.1.1.5
  Metric: 0     IP 172.3.55.0/24
  Metric: 10    IP 172.6.1.0/24
  Metric: 10    IP 172.7.0.0/24
  Metric: 10    IS router-11.00
  Metric: 10    IS router-11.01
router-11.00-00 * 0x0000000b   0x8074460    1161          0/0/0
  Area Address: 49
  NLPID:        0xcc
  Hostname:     router-11
  IP Address:   172.1.11.11
  Metric: 0     IP 172.1.111.0/24
  Metric: 10    IP 172.6.1.0/24
  Metric: 10    IP 172.7.0.0/24
  Metric: 10    IS router-11.01
  Metric: 10    IS router-5.00
router-11.01-00 * 0x00000001   0x80770ec    457           0/0/0
  Metric: 0     IS router-11.00
  Metric: 0     IS router-5.00

```

```
Total LSP count: 3 (L1: 3, L2 0, local L1: 2, local L2 0)
```

```
IS-IS isp (Level-2) Link State Database
```

```

LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
router-5.00-00  0x00000005   0x807997c    457           0/0/0
  Area Address: 49
  NLPID:        0xcc
  Hostname:     router-5
  IP Address:   172.6.1.5
  Metric: 0     IP 172.3.55.0/24
  Metric: 10    IP 172.6.1.0/24
  Metric: 10    IP 172.1.0.0/24
  Metric: 10    IS router-11.00
  Metric: 10    IS router-11.01
  Metric: 10    IP 172.8.111.0/24

```


R3.3 Beta Draft—Cisco Confidential Information

```

router-11.00-00 * 0x0000000d 0x807997c 1184 0/0/0
  Area Address: 49
  NLPID: 0xcc
  Hostname: router-11
  IP Address: 172.28.111.111
  Metric: 0 IP 172.8.111.0/24
  Metric: 10 IP 172.6.1.0/24
  Metric: 10 IP 172.7.0.0/24
  Metric: 10 IS router-11.01
  Metric: 10 IS router-5.00
  Metric: 10 IP 172.3.55.0/24
router-gsr11.01-00 * 0x00000001 0x80770ec 457 0/0/0
  Metric: 0 IS router-11.00
  Metric: 0 IS router-5.00

Total LSP count: 3 (L1: 0, L2 3, local L1: 0, local L2 2)

```

As the output shows, besides the information displayed with the **show isis database** command, the command with the **detail** keyword displays the contents of each LSP.

Table 45 describes the significant fields shown in the display.

Table 45 *show isis instance isp database detail Field Descriptions*

Field	Description
LSPID	LSP identifier. The first six octets form the system ID of the router that originated the LSP. The next octet is the pseudonode ID. When this byte is zero, the LSP describes links from the system. When it is nonzero, the LSP is a so-called nonpseudonode LSP. This is similar to a router link-state advertisement (LSA) in the Open Shortest Path First (OSPF) protocol. The LSP describes the state of the originating router. For each LAN, the designated router for that LAN creates and floods a pseudonode LSP, describing all systems attached to that LAN. The last octet is the LSP number. If there is more data than can fit in a single LSP, the LSP is divided into multiple LSP fragments. Each fragment has a different LSP number. An asterisk (*) indicates that the LSP was originated by the system on which this command is issued.
LSP Seq Num	Sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
LSP Checksum	Checksum of the entire LSP packet.
LSP Holdtime	Amount of time the LSP remains valid (in seconds). An LSP hold time of zero indicates that this LSP was purged and is being removed from the link-state database (LSDB) of all routers. The value indicates how long the purged LSP stays in the LSDB before being completely removed.

R3.3 Beta Draft—Cisco Confidential Information

Table 45 *show isis instance isp database detail Field Descriptions (continued)*

Field	Description
ATT/P/OL	ATT—Attach bit. This bit indicates that the router is also a Level 2 router, and it can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers use the Attach bit to find the closest Level 2 router. They point to a default route to the closest Level 2 router. P—P bit. Detects if the intermediate system is area partition repair capable. Cisco and other vendors do not support area partition repair. OL—Overload bit. Determines if the IS is congested. If the Overload bit is set, other routers do not use this system as a transit router when calculating routes. Only packets for destinations directly connected to the overloaded router are sent to this router.
Area Address	Reachable area addresses from the router. For Level 1 LSPs, these are the area addresses configured manually on the originating router. For Level 2 LSPs, these are all the area addresses for the area this route belongs to.
NLPID	Network Layer Protocol Identifier.
Hostname	Hostname of the node.
IP Address:	Address of the node.
Metric:	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system (ES), or a Connectionless Network Service (CLNS) prefix).

The following is additional sample output from the **show isis database detail** command. This is a Level 2 LSP. The area address 39.0001 is the address of the area in which the router resides.

```
RP/0/RP0/CPU0:router# show isis database level 2 detail
```

```
IS-IS Level-2 Link State Database
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.1111.00-00* 0x00000006   0x4DB3        1194          0/0/0
  Area Address: 39.0001
    NLPID:      0x81 0xCC
    IP Address: 172.18.1.17
    Metric: 10  IS 0000.0C00.1111.09
    Metric: 10  IS 0000.0C00.1111.08
    Metric: 10  IP 172.17.4.0 255.255.255.0
    Metric: 10  IP 172.18.8.0 255.255.255.0
    Metric: 0   IP-External 10.0.0.0 255.0.0.0
```

The IP entries are the directly connected IP subnets the router is advertising (with associated metrics). The IP-External entry is a redistributed route.

Table 46 describes the significant fields shown in the display.

R3.3 Beta Draft—Cisco Confidential Information**Table 46** *show isis database level 2 detail Field Descriptions*

Field	Description
LSPID	LSP identifier. The first six octets form the system ID of the router that originated the LSP. The next octet is the pseudonode ID. When this byte is zero, the LSP describes links from the system. When it is nonzero, the LSP is a so-called nonpseudonode LSP. This is similar to a router link-state advertisement (LSA) in the Open Shortest Path First (OSPF) protocol. The LSP describes the state of the originating router. For each LAN, the designated router for that LAN creates and floods a pseudonode LSP, describing all systems attached to that LAN. The last octet is the LSP number. If there is more data than can fit in a single LSP, the LSP is divided into multiple LSP fragments. Each fragment has a different LSP number. An asterisk (*) indicates that the LSP was originated by the system on which this command is issued.
LSP Seq Num	Sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
LSP Checksum	Checksum of the entire LSP packet.
LSP Holdtime	Time the LSP remains valid (in seconds). An LSP hold time of zero indicates that this LSP was purged and is being removed from the link-state database (LSDB) of all routers. The value indicates how long the purged LSP stays in the LSDB before being completely removed.
ATT/P/OL	ATT—Attach bit. This bit indicates that the router is also a Level 2 router, and it can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers use the Attach bit to find the closest Level 2 router. They point to a default route to the closest Level 2 router. P—P bit. Detects if the intermediate system is area partition repair capable. Cisco and other vendors do not support area partition repair. OL—Overload bit. Determines if the IS is congested. If the Overload bit is set, other routers do not use this system as a transit router when calculating routers. Only packets for destinations directly connected to the overloaded router are sent to this router.
Area Address	Reachable area addresses from the router. For Level 1 LSPs, these are the area addresses configured manually on the originating router. For Level 2 LSPs, these are all the area addresses for the area to which this route belongs.
NLPID	Network Layer Protocol Identifier.
Hostname	Hostname of the node.
IP Address:	IP address of the node.
Metric:	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system (ES), or a Connectionless Network Service (CLNS) prefix).

R3.3 Beta Draft—Cisco Confidential Information

show isis database-log

To display the entries in the Intermediate System-to-Intermediate System (IS-IS) database log, use the **show isis database-log** command in EXEC mode.

show isis database-log [**last** *number* | **first** *number* | **level** {**1** | **2**}]

Syntax Description	last <i>number</i>	(Optional) Specifies that the output is restricted to the last <i>number</i> of entries.
	first <i>number</i>	(Optional) Specifies that the output is restricted to the first <i>number</i> of entries.
	level { 1 2 }	(Optional) Displays the database log for Level 1 or Level 2 independently.

Defaults Both Level 1 and Level 2 are configured if no level is specified.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	isis	read

Examples The following is sample output from the **show isis database-log** command:

```
RP/0/RP0/CPU0:router# show isis database-log
```

```
IS-IS 10 Level 1 Link State Database Log
                                New LSP                                Old LSP
WHEN      LSPID                  Op  Seq Num    Holdtime OL  Seq Num    Holdtime OL
01:17:19  12b1.03-00             REP  0x00000003  1200      0  0x00000002  340      0
001:06:20  12b1.00-00             REP  0x000001d8  1200      0  0x000001d7  375      0
01:06:00  12b1.03-00             REP  0x00000004  1200      0  0x00000003  520      0
01:05:46  12a1.00-00             REP  0x000001fc  1200      0  0x000001fb  425      0
```

R3.3 Beta Draft—Cisco Confidential Information

```

00:55:01 12b1.00-00      REP 0x000001d9 1200      0 0x000001d8 520      0
00:53:39 12b1.03-00      REP 0x00000005 1200      0 0x00000004 459      0
00:53:19 12a1.00-00      REP 0x000001fd 1200      0 0x000001fc 453      0
00:42:12 12b1.00-00      REP 0x000001da 1200      0 0x000001d9 431      0
00:39:56 12b1.03-00      REP 0x00000006 1200      0 0x00000005 376      0
00:38:54 12a1.00-00      REP 0x000001fe 1200      0 0x000001fd 334      0
00:29:10 12b1.00-00      REP 0x000001db 1200      0 0x000001da 418      0
00:27:22 12b1.03-00      REP 0x00000007 1200      0 0x00000006 446      0
00:25:10 12a1.00-00      REP 0x000001ff 1200      0 0x000001fe 375      0
00:17:04 12b1.00-00      REP 0x000001dc 1200      0 0x000001db 473

```

Table 47 describes the significant fields shown in the display.

Table 47 *show isis database-log Field Descriptions*

Field	Description
WHEN	Elapsed time (in hh:mm:ss) since the event was logged.
LSPID	LSP identifier. The first six octets form the system ID of the router that originated the LSP. The next octet is the pseudonode ID. When this byte is zero, the LSP describes links from the system. When it is nonzero, the LSP is a so-called nonpseudonode LSP. This is similar to a router link-state advertisement (LSA) in the Open Shortest Path First (OSPF) protocol. The LSP describes the state of the originating router. For each LAN, the designated router for that LAN creates and floods a pseudonode LSP, describing all systems attached to that LAN. The last octet is the LSP number. If there is more data than can fit in a single LSP, the LSP is divided into multiple LSP fragments. Each fragment has a different LSP number. An asterisk (*) indicates that the LSP was originated by the system on which this command is issued.
New LSP	New router or pseudonode appearing in the topology.
Old LSP	Old router or pseudonode leaving the topology.
Op	Operation on the database: inserted (INS) or replaced (REP).
Seq Num	Sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
Holdtime	Time the LSP remains valid (in seconds). An LSP hold time of zero indicates that this LSP was purged and is being removed from the link-state database (LSDB) of all routers. The value indicates how long the purged LSP stays in the LSDB before being completely removed.
OL	Overload bit. Determines if the IS is congested. If the Overload bit is set, other routers do not use this system as a transit router when calculating routers. Only packets for destinations directly connected to the overloaded router are sent to this router.

Related Commands

Command	Description
show isis database	Displays the IS-IS link-state packet (LSP) database.

R3.3 Beta Draft—Cisco Confidential Information

show isis hostname

To display the entries in the Intermediate System-to-Intermediate System (IS-IS) router name-to-system ID mapping table, use the **show isis hostname** command in EXEC mode.

show isis [*instance instance-id*] **hostname**

Syntax Description

instance *instance-id* (Optional) Displays the IS-IS router name-to-system ID mapping table for the specified IS-IS instance only.

The *instance-id* argument is the instance identifier (alphanumeric) defined by the **router isis** command.

Defaults

No instance ID specified displays the IS-IS router name-to-system ID mapping table for all the IS-IS instances.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **show isis hostname** command does not display entries if the dynamic hostnames are disabled.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis hostname** command with the **instance** and *instance-id* values specified:

```
RP/0/RP0/CPU0:router# show isis instance isp hostname

ISIS isp hostnames
Level  System ID      Dynamic Hostname
 1      0001.0000.0005 router-5
 2      * 0001.0000.0011 router-11
```

R3.3 Beta Draft—Cisco Confidential Information

Table 48 describes the significant fields shown in the display.

Table 48 *show isis instance isp hostname Field Descriptions*

Field	Description
Level	IS-IS level of the router.
System ID	Dynamic hostname of the system. The hostname is specified using the hostname command. If the dynamic hostname is not known or hostname dynamic disable command has been executed, the 6-octet system ID is used.
Dynamic Hostname	Hostname of the router.
*	Local router.

Related Commands

Command	Description
hostname	Specifies the name of the local router.
hostname dynamic disable	Enables the IS-IS routing protocol to dynamically update the mapping of router names to system IDs.

R3.3 Beta Draft—Cisco Confidential Information

show isis interface

To display information about the Intermediate System-to-Intermediate System (IS-IS) interfaces, use the **show isis interface** command in EXEC mode.

show isis interface [*type instance* | **level** {**1** | **2**}] [**brief**]

Syntax Description

<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>instance</i>	(Optional) Either a physical interface instance or a virtual interface instance as follows: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
level { 1 2 }	(Optional) Displays IS-IS interface information for Level 1 or Level 2 independently.
brief	(Optional) Displays brief interface output.

Defaults

Displays all IS-IS interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Release	Modification
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis interface** command without any keywords:

```
RP/0/RP0/CPU0:router# show isis interface

IS-IS 1 Interfaces
GigabitEthernet0/6/0/0      Enabled
  Adjacency Formation:      Enabled
  Prefix Advertisement:     Enabled
  BFD:                      Disabled
  BFD Min Interval:         150
  BFD Multiplier:           3

Circuit Type:                level-1-2
Media Type:                  LAN
Circuit Number:              1

Level-1
  Adjacency Count:           1
  LAN ID:                    12a5.01
  Priority (Local/DIS):       64/64
  Next LAN IIH in:           7 s
  LSP Pacing Interval:       33 ms
Level-2
  Adjacency Count:           1
  LAN ID:                    12a5.01
  Priority (Local/DIS):       64/64
  Next LAN IIH in:           7 s
  LSP Pacing Interval:       33 ms

CLNS I/O
  Protocol State:            Up
  MTU:                       1497
  SNPA:                      0004.2892.4af4
  Layer-2 MCast Groups Membership:
    All Level-1 ISs:         Yes
    All Level-2 ISs:         Yes

IPv4 Unicast Topology:       Enabled
  Adjacency Formation:       Running
  Prefix Advertisement:       Running
  Metric (L1/L2):            10/10
  MPLS LDP Sync (L1/L2):     Enabled/Enabled
  Sync Status:               Not Achieved
```

R3.3 Beta Draft—Cisco Confidential Information

```

IPv4 Address Family:      Enabled
Protocol State:           Up
Forwarding Address(es):   11.0.0.13
Global Prefix(es):        11.0.0.0/24

LSP transmit timer expires in 0 ms
LSP transmission is idle
Can send up to 9 back-to-back LSPs in the next 0 ms

```

Table 49 describes the significant fields shown in the display.

Table 49 *show isis interface Field Descriptions*

Field	Description
GigabitEthernet0/6/0/0	Status of the interface, either enabled or disabled.
Adjacency formation:	Status of adjacency formation, either enabled or disabled.
Prefix Advertisement:	Status of advertising connected prefixes, either enabled or disabled.
BFD:	Status of Bidirectional Forwarding Detection (BFD), either enabled or disabled.
BFD Min Interval:	BFD minimum interval.
BFD Multiplier:	BFD multiplier.
Circuit Type:	Levels the interface is running on (circuit-type configuration) which may be a subset of levels on the router.
Media Type:	Media type on which IS-IS is running.
Circuit Number:	Unique ID assigned to a circuit internally (8-bit integer).
Extended Circuit Number:	Valid only for point-to-point interfaces (32-bit integer).
Adjacency Count:	Number of adjacencies formed with a neighboring router that supports the same set of protocols.
LAN ID:	ID of the LAN.
Priority (Local/DIS):	Priority of this interface or priority of the Designated Intermediate System.
Next LAN IIH in:	Time (in seconds) in which the next LAN hello message is sent.
LSP Pacing Interval:	Interval at which the link-state packet (LSP) transmission rate (and by implication the reception rate of other systems) is to be reduced.
Protocol State:	Running state of the protocol.
MTU:	Link maximum transmission unit (MTU).
SNPA:	Data-link address (also known as the Subnetwork Point of Attachment [SNPA]) of the neighbor.
All Level-n ISs:	Status of interface membership in Layer 2 multicast group.
IPv4 Unicast Topology:	Status of the topology, either enabled or disabled.
Adjacency Formation:	Status of adjacency formation.
Prefix Advertisement:	Status of advertising prefixes, either enabled or disabled.

R3.3 Beta Draft—Cisco Confidential Information

Table 49 *show isis interface Field Descriptions (continued)*

Field	Description
Metric (L1/L2):	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system (ES), or a connectionless network service (CLNS) prefix).
MPLS LDP Sync (L1/L2)	Status of LDP IS-IS synchronization, either enabled or disabled. When enabled, the state of synchronization (Sync Status) is additionally displayed as either achieved or not achieved.
IPv4 Address Family:	Status of the address family, either enabled or disabled.
Protocol State:	State of the protocol.
Forwarding Address(es):	Addresses on this interface used by the neighbor for next-hop forwarding.
Global Prefix(es):	Prefixes for this interface included in the LSP.
LSP transmit timer expires in	LSP transmission expiration timer interval (in milliseconds).
LSP transmission is	State of LSP transmission priority.

The following is sample output from the **show isis interface** command with the **brief** keyword:

```
RP/0/0/CPU0:router# show isis interface brief
```

Interface	All OK	Adjs L1 L2	Adj Topos Run/Cfg	Adv Topos Run/Cfg	CLNS	MTU	Prio L1 L2
PO0/5/0/0	Yes	1 1	1/1	1/1	Up	4469	- -
Gi0/6/0/0	Yes	1* 1*	1/1	1/1	Up	1497	64 64

Table 50 describes the significant fields shown in the display.

Table 50 *show isis interface brief Field Descriptions*

Field	Description
Interface	Name of the interface.
All OK	Everything is working as expected for this interface.
Adjs L1 L2	Number of L1 and L2 adjacencies over this interface.
Adj Topos Run/Cfg	Number of topologies that participate in forming adjacencies. Number of topologies that were configured to participate in forming adjacencies.
Adv Topos Run/Cfg	Number of topologies that participate in advertising prefixes. Number of topologies that were configured to participate in advertising prefixes.
CLNS	Status of the Connectionless Network Service.
MTU	Maximum transfer unit size for the interface.
Prio L1 L2	Interface L1 priority. Interface L2 priority.

R3.3 Beta Draft—Cisco Confidential Information

show isis lsp-log

To display link-state packet (LSP) log information, use the **show isis lsp-log** command in EXEC mode.

show isis [*instance instance-id*] **lsp-log** [*last number* | *first number* | **level** {**1** | **2**}]

Syntax Description	instance <i>instance-id</i>	(Optional) Displays the LSP log information for the specified IS-IS instance only. The <i>instance-id</i> argument is the instance identifier (alphanumeric) defined by the router isis command.
	last <i>number</i>	(Optional) Specifies that the output is restricted to the last <i>number</i> of entries.
	first <i>number</i>	(Optional) Specifies that the output is restricted to the first <i>number</i> of entries.
	level { 1 2 }	(Optional) Displays the Intermediate System-to-Intermediate System (IS-IS) link-state database for Level 1 or Level 2 independently.

Defaults

No instance ID specified displays the LSP log information for all the IS-IS instances. Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	isis	read

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following is sample output from the **show isis lsp-log** command with the **instance** and *instance-id* values specified:

```
RP/0/RP0/CPU0:router# show isis instance isp lsp-log
```

```
ISIS isp Level 1 LSP log
  When      Count      Interface      Triggers
00:02:36    1
00:02:31    1
00:02:26    1      PO4/1      LSPREGEN
00:02:24    1      PO4/1      DELADJ
00:02:23    1      Gi5/0      NEWADJ
00:02:23    1      Gi5/0      DIS
00:01:27    1      Lo0        IPDOWN
00:01:12    1      Lo0        IPUP
```

```
ISIS isp Level 2 LSP log
  When      Count      Interface      Triggers
00:02:36    1
00:02:30    1
00:02:26    1      PO4/1      LSPREGEN
00:02:24    1      PO4/1      DELADJ
00:02:24    1      PO4/1      NEWADJ
00:02:23    1      Gi5/0      DIS
00:02:21    1
00:02:21    1
00:01:27    1      Lo0        AREASET
00:01:27    1      Lo0        IPDOWN
00:01:12    1      Lo0        IPUP
```

[Table 51](#) describes the significant fields shown in the display.

Table 51 *show isis instance isp lsp-log Field Descriptions*

Field	Description
Level	IS-IS level of the router.
When	How long ago (in hh:mm:ss) an LSP rebuild occurred. The last 20 occurrences are logged.
Count	Number of events that triggered this LSP run. When there is a topology change, often multiple LSPs are received in a short period. A router waits 5 seconds before running a full LSP, so it can include all new information. This count denotes the number of events (such as receiving new LSPs) that occurred while the router was waiting its 5 seconds before running full LSP.

R3.3 Beta Draft—Cisco Confidential Information

Table 51 *show isis instance isp lsp-log Field Descriptions (continued)*

Field	Description
Interface	Interface that corresponds to the triggered reasons for the LSP rebuild.
Triggers	A list of all reasons that triggered an LSP rebuild. The triggers are: • AREASET—area set changed • ATTACHFLAG—bit attached • CLEAR—clear command • CONFIG—configuration change • DELADJ—adjacency deleted • DIS—DIS changed • IFDOWN—interface down • IPADDRCHG—IP address change • IPDEFORIG—IP def-orig • IPDOWN—connected IP down • IFDOWN—interface down • IPEXT—external IP • IPIA—interarea IP • IPUP—connected IP up • LSPDBOL—LSPDBOL bit • LSPREGEN—LSP regeneration • NEWADJ—new adjacency

R3.3 Beta Draft—Cisco Confidential Information

show isis mesh-group

To display Intermediate System-to-Intermediate System (IS-IS) mesh group information, use the **show isis mesh-group** command in EXEC mode.

show isis [**instance** *instance-id*] **mesh-group**

Syntax Description

instance <i>instance-id</i>	(Optional) Displays the mesh group information for the specified IS-IS instance only. The <i>instance-id</i> argument is the instance identifier (alphanumeric) defined by the router isis command.

Defaults

No instance ID specified displays the IS-IS mesh group information for all the IS-IS instances.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis mesh-group** command with the **instance** and *instance-id* values specified:

```
RP/0/RP0/CPU0:router# show isis instance isp mesh-group

ISIS isp Mesh Groups

Mesh group 6:
POS0/4/0/1
```

R3.3 Beta Draft—Cisco Confidential Information

Table 52 describes the significant fields shown in the display.

Table 52 *show isis instance isp mesh-group Field Descriptions*

Field	Description
Mesh group	Mesh group number to which this interface is a member. A mesh group optimizes link-state packet (LSP) flooding in nonbroadcast multiaccess (NBMA) networks with highly meshed, point-to-point topologies. LSPs that are first received on interfaces that are part of a mesh group are flooded to all interfaces except those in the same mesh group.
POS0/4/0/1	Interface belonging to mesh group 6.

R3.3 Beta Draft—Cisco Confidential Information

show isis mpls traffic-eng adjacency-log

To display a log of Multiprotocol Label Switching traffic engineering (MPLS TE) adjacency changes for an Intermediate System-to-Intermediate System (IS-IS) instance, use the **show isis mpls traffic-eng adjacency-log** command in EXEC mode.

show isis [**instance** *instance-id*] **mpls traffic-eng adjacency-log** [**last number** | **first number**]

Syntax Description	instance <i>instance-id</i>	(Optional) Displays the MPLS TE adjacency changes for the specified IS-IS instance only. The <i>instance-id</i> argument is the instance identifier (alphanumeric) defined by the router isis command.
	last number	(Optional) Specifies that the output is restricted to last <i>number</i> of entries.
	first number	(Optional) Specifies that the output is restricted to last <i>number</i> of entries.

Defaults	No instance ID specified displays MPLS TE adjacency changes for all the IS-IS instances.

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The last number and first number keywords and arguments were added.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the show isis mpls traffic-eng adjacency-log command to display the status of MPLS TE adjacencies.

Task ID	Task ID	Operations
	isis	read

```
show isis mpls traffic-eng adjacency-log
```

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following is sample output from the **show isis mpls traffic-eng adjacency-log** command with the **instance** and *instance-id* values specified:

```
RP/0/RP0/CPU0:router# show isis instance isp mpls traffic-eng adjacency-log

IS-IS isp Level-2 MPLS Traffic Engineering adjacency log
When      Neighbor ID      IP Address      Interface Status
00:03:36  router-6         172.17.1.6      PO0/3/0/1 Up
00:03:36  router-6         172.17.1.6      PO0/3/0/1 Down
00:02:38  router-6         172.17.1.6      PO0/3/0/1 Up
```

Table 53 describes the significant fields shown in the output.

Table 53 *show isis instance isp mpls traffic-eng adjacency-log Field Descriptions*

Field	Description
When	Time (in hh:mm:ss) since the entry was recorded in the log.
Neighbor ID	Identification value of the neighbor.
IP Address	Neighbor IP Version 4 (IPv4) address.
Interface	Interface from which a neighbor is learned.
Status	Up (active) or Down (disconnected).

Related Commands

Command	Description
show isis mpls traffic-eng advertisements	Displays the last flooded record from MPLS traffic engineering.

R3.3 Beta Draft—Cisco Confidential Information

show isis mpls traffic-eng advertisements

To display the latest flooded record from Multiprotocol Label Switching traffic engineering (MPLS TE) for an Intermediate System-to-Intermediate System (IS-IS) instance, use the **show isis mpls traffic-eng advertisements** command in EXEC mode.

show isis [*instance instance-id*] **mpls traffic-eng advertisements**

Syntax Description	instance <i>instance-id</i>	(Optional) Displays the latest flooded record from MPLS TE for the specified IS-IS instance only. The <i>instance-id</i> argument is the instance identifier (alphanumeric) defined by the router isis command.

Defaults	No instance ID specified displays the latest flooded record from MPLS TE for all the IS-IS instances.

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the show isis mpls traffic-eng advertisements command to verify that MPLS TE is flooding its record and that the bandwidths are correct.

Task ID	Task ID	Operations
	isis	read

Examples	The following is sample output from the show isis mpls traffic-eng advertisements command with the instance and <i>instance-id</i> values specified:

```
RP/0/RP0/CPU0:router# show isis instance isp mpls traffic-eng advertisements
```

```
ISIS isp Level-2 MPLS Traffic Engineering advertisements
  System ID: router-9
  Router ID: 172.18.0.9
  Link Count: 1
```

R3.3 Beta Draft—Cisco Confidential Information

```

Link[0]
  Neighbor System ID: router-gsr6 (P2P link)
  Interface IP address: 172.18.0.9
  Neighbor IP Address: 172.18.0.6
  Admin. Weight: 0
  Physical BW: 155520000 bits/sec
  Reservable BW global: 10000000 bits/sec
  Reservable BW sub: 0 bits/sec
  Global pool BW unreserved:
    [0]: 10000000 bits/sec, [1]: 10000000 bits/sec
    [2]: 10000000 bits/sec, [3]: 10000000 bits/sec
    [4]: 10000000 bits/sec, [5]: 10000000 bits/sec
    [6]: 10000000 bits/sec, [7]: 10000000 bits/sec
  Sub pool BW unreserved:
    [0]: 0 bits/sec, [1]: 0 bits/sec
    [2]: 0 bits/sec, [3]: 0 bits/sec
    [4]: 0 bits/sec, [5]: 0 bits/sec
    [6]: 0 bits/sec, [7]: 0 bits/sec
  Affinity Bits: 0x00000000

```

Table 54 describes the significant fields shown in the output.

Table 54 *show isis instance isp mpls traffic-eng advertisements Field Descriptions*

Field	Description
System ID	Dynamic hostname of the system. The hostname is specified using the hostname command. If the dynamic hostname is not known or hostname dynamic disable command has been executed, the 6-octet system ID is used.
Router ID	MPLS TE router ID.
Link Count	Number of links that MPLS TE advertised.
Neighbor System ID	System ID of a neighbor number in an area. The six bytes directly preceding the n-selector are the system ID. The system ID length is a fixed size and cannot be changed. The system ID must be unique throughout each area (Level 1) and throughout the backbone (Level 2). In an IS-IS routing domain, each router is represented by a 6-byte hexadecimal system ID. When network administrators maintain and troubleshoot networking devices, they must know the router name and corresponding system ID.
Interface IP address	IP address of the interface.
Neighbor IP Address	IP address of the neighbor.
Admin. Weight	Administrative weight associated with this link.
Physical BW	Link bandwidth capacity (in bits per second).
Reservable BW	Reservable bandwidth on this link.
Global pool BW unreserved	Unreserved bandwidth that is available in the global pool.
Sub pool BW unreserved	Amount of unreserved bandwidth that is available in the subpool.
Affinity Bits	Link attribute flags being flooded.

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	show isis mpls traffic-eng adjacency-log	Displays a log of MPLS TE adjacency changes for IS-IS.

R3.3 Beta Draft – Cisco Confidential Information

show isis mpls traffic-eng tunnel

To display Multiprotocol Label Switching traffic engineering (MPLS TE) tunnel information for an Intermediate System-to-Intermediate System (IS-IS) instance, use the **show isis mpls traffic-eng tunnel** command in EXEC mode.

show isis [*instance instance-id*] **mpls traffic-eng tunnel**

Syntax Description	instance <i>instance-id</i>	(Optional) Displays the MPLS TE tunnel information for the specified IS-IS instance only. The <i>instance-id</i> argument is the instance identifier (alphanumeric) defined by the router isis command.

Defaults	No instance ID specified displays the MPLS TE tunnel information for all the IS-IS instances.

Command Modes	EXEC

Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>Release 2.0</td><td>This command was introduced on the Cisco CRS-1.</td></tr><tr><td>Release 3.0</td><td>No modification.</td></tr><tr><td>Release 3.2</td><td>This command was supported on the Cisco XR 12000 Series Router.</td></tr><tr><td>Release 3.3</td><td>No modification.</td></tr></table>	Release	Modification	Release 2.0	This command was introduced on the Cisco CRS-1.	Release 3.0	No modification.	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.	Release 3.3	No modification.
Release	Modification										
Release 2.0	This command was introduced on the Cisco CRS-1.										
Release 3.0	No modification.										
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.										
Release 3.3	No modification.										

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the show isis command to find the current status of MPLS TE tunnels. Tunnels are used in IS-IS next-hop calculations.

Task ID	<table><tr><th>Task ID</th><th>Operations</th></tr><tr><td>isis</td><td>read</td></tr></table>	Task ID	Operations	isis	read
Task ID	Operations				
isis	read				

Examples	The following is sample output from the show isis mpls traffic-eng tunnel command: <pre>RP/0/RP0/CPU0:router# show isis mpls traffic-eng tunnel ISIS isp Level-2 MPLS Traffic Engineering tunnels System Id Tunnel Name Bandwidth Nexthop Metric Mode router-6 tu0 100000 172.18.1.6 0 Relative</pre>

R3.3 Beta Draft—Cisco Confidential Information

Table 55 describes the significant fields shown in the output.

Table 55 *show isis mpls traffic-eng tunnel Field Descriptions*

Field	Description
System ID	Dynamic hostname of the system. The hostname is specified using the hostname command. If the dynamic hostname is not known or hostname dynamic disable command has been executed, the 6-octet system ID is used.
Tunnel Name	Name of the MPLS TE tunnel interface.
Bandwidth	MPLS TE-specified tunnel bandwidth of the tunnel.
Nexthop	MPLS TE destination IP address of the tunnel.
Metric	MPLS TE metric of the tunnel.
Mode	MPLS TE metric mode of the tunnel. It can be relative or absolute.

R3.3 Beta Draft—Cisco Confidential Information

show isis neighbors

To display information about Intermediate System-to-Intermediate System (IS-IS) neighbors, use the **show isis neighbors** command in EXEC mode.

show isis [**instance** *instance-id*] **neighbors** [*interface-type interface-number*] [**summary**] [**detail**]
[**systemid** *system-id*]

Syntax Description		
instance <i>instance-id</i>	(Optional) Displays the IS-IS neighbor information for the specified IS-IS instance only.	The <i>instance-id</i> argument is the instance identifier (alphanumeric) defined by the router isis command.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.	
<i>interface-number</i>	(Optional) Interface number. For more information about the numbering syntax for the router, use the question mark (?) online help function. No space is required between the <i>interface-type</i> and <i>interface-number</i> values.	
summary	(Optional) Displays neighbor status count for each level.	
detail	(Optional) Displays additional details.	
systemid <i>system-id</i>	(Optional) Displays the information for the specified neighbor only.	

Defaults No instance ID specified displays neighbor information for all the IS-IS instances. Both Level 1 and Level 2 are configured if no level is specified.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	isis	read

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following is sample output from the **show isis neighbors** command with the **instance** and **instance-id** values specified:

```
RP/0/RP0/CPU0:router# show isis instance isp neighbors detail
```

```
ISIS isp neighbors:
```

System ID	Interface	SNPA	State	Holdtime	Type	IETF-NSF
router-5	PO4/1	*PtoP*	Up	24	L1L2	Capable
Area Address(es): 49						
IPv4 Address(es): 172.18.1.5*						
Topologies: 'IPv4 Unicast'						
Uptime: 00:09:30						
router-5	Gi5/0	0003.6cff.0680	Up	23	L1L2	Capable
Area Address(es): 49						
IPv4 Address(es): 172.36.0.5*						
Topologies: 'IPv4 Unicast'						
Uptime: 00:09:21						

```
Total adjacency count: 4
```

Table 56 describes the significant fields shown in the display.

Table 56 *show isis instance isp neighbors Field Descriptions*

Field	Description
System ID	Dynamic hostname of the system. The hostname is specified using the hostname command. If the dynamic hostname is not known or hostname dynamic disable command has been executed, the 6-octet system ID is used.
Interface	Interface through which the neighbor is reachable.
SNPA	Data-link address (also known as the Subnetwork Point of Attachment [SNPA]) of the neighbor.
State	State of the neighboring interface.
Holdtime	Hold time of the neighbor.
Type	Type of adjacency.
IETF-NSF	Specifies whether the neighbor can adhere to the IETF-NSF restart mechanism.
Area Address(es)	Number of area addresses on this router.
IPv4 Address(es)	IPv4 addresses configured on this router.
Topologies	Address and subaddress families for which IS-IS is configured.
Uptime	Time (in hh:mm:ss) that the neighbor has been up.

The following is sample output from the **show isis neighbors** command with the **summary** keyword specified:

```
RP/0/RP0/CPU0:router# show isis instance isp neighbors summary
```

```
ISIS isp neighbor summary:
```

State	L1	L2	L1L2
Up	0	0	2
Init	0	0	0
Failed	0	0	0

R3.3 Beta Draft – Cisco Confidential Information

Table 57 describes the significant fields shown in the display.

Table 57 *show isis neighbors summary Field Descriptions*

Field	Description
State	State of the neighbor is up, initialized, or failed.
L1	Number of Level 1 neighbors.
L2	Number of Level 2 neighbors.
L1L2	Number of Level 1 and 2 neighbors.

Related Commands

Command	Description
show isis adjacency	Displays IS-IS adjacencies.

R3.3 Beta Draft—Cisco Confidential Information

show isis protocol

To display summary information about an Intermediate System-to-Intermediate System (IS-IS) instance, use the **show isis protocol** command in EXEC mode.

show isis [*instance instance-id*] **protocol**

Syntax Description	instance <i>instance-id</i>	(Optional) Displays the IS-IS adjacencies for the specified IS-IS instance only. The <i>instance-id</i> argument is the instance identifier (alphanumeric) defined by the router isis command.

Defaults	No instance ID specified displays IS-IS adjacencies for all the IS-IS instances.

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	isis	read

Examples	The following is sample output from the show isis protocol command:

```
RP/0/RP0/CPU0:router# show isis protocol
```

```
IS-IS Router: isp
System Id: 0001.0000.0011
IS Levels: level-1-2
Manual area address(es):
  49
Routing for area address(es):
  49
Non-stop forwarding: Cisco Proprietary NSF Restart enabled
Process startup mode: Cold Restart
```

R3.3 Beta Draft—Cisco Confidential Information

```

Topologies supported by IS-IS:
  IPv4 Unicast
    Level-1 iSPF status: Dormant (awaiting initial convergence)
    Level-2 iSPF status: Dormant (awaiting initial convergence)
    No protocols redistributed
    Distance: 115
Interfaces supported by IS-IS:
  Loopback0 is running passively (passive in configuration)
  POS0/4/0/1 is running actively (active in configuration)
  POS0/5/0/1 is running actively (active in configuration)

```

Table 58 describes the significant fields shown in the display.

Table 58 *show isis protocol Field Descriptions*

Field	Description
System ID:	Dynamic hostname of the system. The hostname is specified using the hostname command. If the dynamic hostname is not known or hostname dynamic disable command has been executed, the 6-octet system ID is used.
IS Levels:	IS-IS level of the router.
Manual area address(es)	Area addresses that are manually configured.
Routing for area address(es)	Area addresses for which this router provides the routing.
Non-stop forwarding:	Status and name of nonstop forwarding (NSF).
Process startup mode:	Mode in which the last process startup occurred.
iSPF status:	State of incremental shortest path first (iSPF) configuration for this IS-IS instance. Four states exist: Disabled if iSPF has not been configured but is awaiting a full SPF to compile the topology for use by the iSPF algorithm. Dormant if iSPF has been configured but is awaiting initial convergence before initializing. Awake if iSPF has been configured but is awaiting a full SPF to compile the topology for use by the iSPF algorithm. Active if IS-IS is ready to consider using the iSPF algorithm whenever a new route calculation needs to be run.
No protocols redistributed:	No redistributed protocol information exists to be displayed.
Distance:	Administrative distance for this protocol.

R3.3 Beta Draft—Cisco Confidential Information

show isis route

To display IP reachability information for an Intermediate System-to-Intermediate System (IS-IS) instance, use the **show isis route** command in EXEC mode.

```
show isis [instance instance-id] [ipv4 | ipv6 | afi-all [unicast]] route [ip-address mask
[longer-prefixes]] [backup] [detail]
```

Syntax Description		
instance <i>instance-id</i>	(Optional) Displays the IP reachability information for the specified IS-IS instance only.	The <i>instance-id</i> argument is the instance identifier (alphanumeric) defined by the router isis command.
ipv4	(Optional) Specifies IP Version 4 address prefixes.	
ipv6	(Optional) Specifies IP Version 6 address prefixes.	
afi-all	(Optional) Specifies all address prefixes.	
unicast	(Optional) Specifies unicast address prefixes.	
<i>ip-address</i>	(Optional) Network IP address about which routing information should be displayed.	
<i>mask</i>	(Optional) Network mask specified in either of two ways:	- Network mask can be a four-part, dotted decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit is a network address. - Network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are ones, and the corresponding bits of the address are the network address.
longer-prefixes	(Optional) Displays route and more-specific routes.	
backup	(Optional) Displays backup information for this entry.	
detail	(Optional) Displays link-state packet (LSP) details.	

Defaults No instance ID specified displays the IP reachability information for all the IS-IS instances.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The longer-prefixes keyword was added.
	Release 3.3	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis route** command:

```
RP/0/RP0/CPU0:router# show isis route

ISIS isp IP Topology Table

C - Connected route for IS-IS Interface
L1 - Level 1
L2 - Level 2
ia - Interarea (leaked into Level 1)
df - Level 1 Default (closest L2 router)
R - Redistributed route
su - Summary null route

Maximum parallel path count: 6

C 172.18.0.0/24 is directly connected, POS0/5/0/0
C 172.19.1.0/24 is directly connected, POS0/4/0/1
L1 172.35.0.0/24 [10], via 172.17.11.0, POS0/4/0/1
                        via 172.16.10.0, POS0/5/0/0
C 172.18.0/24 is directly connected, Loopback0
```

Table 59 describes the significant fields shown in the display.

Table 59 *show isis route ipv4 unicast Field Descriptions*

Field	Description
C172.18.0.0/24	Connected route for POS interface 0/5/0/0.
C 172.19.1.0/24	Connected route for POS interface 0/4/0/1.
L1 172.35.0.0/24 [10]	Connected route for Level 1 area.
C 172.18.0/24	Connected route for loopback interface 0.

R3.3 Beta Draft – Cisco Confidential Information

show isis spf-log

To display how often and why the router has run a full shortest path first (SPF) calculation, use the **show isis spf-log** command in EXEC mode.

```
show isis [instance instance-id] [ipv4 | ipv6 | afi-all [unicast]] spf-log [level { 1 | 2}] [ispf | fspf |
prc | nhc] [detail | verbose] [last number | first number]
```

Syntax Description		
instance <i>instance-id</i>	(Optional) Displays the IS-IS SPF log for the specified IS-IS instance only.	
ipv4	(Optional) Specifies IP Version 4 address prefixes.	
ipv6	(Optional) Specifies IP Version 6 address prefixes.	
afi-all	(Optional) Specifies all address prefixes.	
unicast	(Optional) Specifies unicast address prefixes.	
level { 1 2 }	(Optional) Displays the IS-IS SPF log for Level 1 or Level 2 independently.	
ispf	(Optional) Specifies incremental SPF entries only.	
fspf	(Optional) Specifies full SPF entries only.	
prc	(Optional) Specifies partial route calculations only.	
nhc	(Optional) Specifies next hop route calculations only.	
detail	(Optional) Specifies detailed output. Includes a breakdown of the time taken to perform the calculation and changes resulting from the calculation.	
verbose	(Optional) Specifies verbose output.	
last <i>number</i>	(Optional) Specifies that the output is restricted to the last <i>number</i> of entries.	
first <i>number</i>	(Optional) Specifies that the output is restricted to the first <i>number</i> of entries.	

Defaults

No instance ID specified displays IS-IS adjacencies for all the IS-IS instances.
Both Level 1 and Level 2 are configured if no level is specified.
Displays all types of route calculation (not just fspf, ispf and prc).

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	The ispf , fspf , prc , detail , internal , last number and first number keywords and arguments were added.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The internal keyword was removed.
Release 3.3	The nhc and verbose keywords were added.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis spf-log** command:

```
RP/0/RP0/CPU0:router# show isis spf-log
```

```

IS-IS 1 Level 1 IPv4 Unicast Route Calculation Log
      Time  Total Trig
Timestamp  Type (ms)  Nodes Count First Trigger LSP Triggers
-----
--- Thurs Aug 19 2004 ---
12:00:50.787 FSPF 1 1 3 ensoft-grs7.00-00 LSPHEADER TLVCODE
12:00:52.846 FSPF 1 1 1 ensoft-grs7.00-00 LSPHEADER
12:00:56.049 FSPF 1 1 1 ensoft-grs7.00-00 TLVCODE
12:01:02.620 FSPF 1 1 2 ensoft-grs7.00-00 NEWADJ LINKTLV

IS-IS 1 Level 1 IPv4 Unicast Route Calculation Log
      Time  Total Trig
Timestamp  Type (ms)  Nodes Count First Trigger LSP Triggers
-----
--- Mon Aug 19 2004 ---
12:00:50.790 FSPF 0 1 4 ensoft-grs7.00-00 LSPHEADER TLVCODE
12:00:54.043 FSPF 1 1 2 ensoft-grs7.00-00 NEWADJ LSPHEADER
12:00:55.922 FSPF 1 2 1 ensoft-grs7.00-00 NEWLSPO
12:00:56.724 FSPF 1 13 1 ensoft-grs7.00-00 NEWLSPO

```

Table 60 describes the significant fields shown in the output.

Table 60 *show isis spf-log ipv4 unicast Field Descriptions*

Field	Description
Level	IS-IS level of the router.
Timestamp	Time when the SPF calculation started.
Duration	Number of milliseconds taken to complete this SPF run. Elapsed time is wall clock time, not CPU time.
Nodes	Number of routers and pseudonodes (LANs) that make up the topology calculated in this SPF run.
Trig Count	Number of events that triggered this SPF run. When there is a topology change, often multiple link-state packets (LSPs) are received in a short time. Depending on the configuration of the spf-interval command, a router may wait for a fixed period of time before running a router calculation. This count denotes the number of triggering events that occurred while the router was waiting to run the calculation. For a full description of the triggering events, see Table 61.

R3.3 Beta Draft—Cisco Confidential Information

Table 60 *show isis spf-log ipv4 unicast Field Descriptions (continued)*

Field	Description
First Trigger LSP	LSP ID stored by the router whenever a full SPF calculation is triggered by the arrival of a new LSP. The LSP ID can suggest the source of routing instability in an area. If multiple LSPs are causing an SPF run, only the LSP ID of the first received LSP is remembered.
Triggers	List of all reasons that triggered a full SPF calculation. For a list of possible triggers, see Table 61 .

[Table 61](#) lists triggers of a full SPF calculation.

Table 61 *List of Triggers*

Trigger	Description
PERIODIC	Runs a full SPF calculation every 15 minutes.
NEWLEVEL	Configured new level (using is-type) on this router.
RTCLEARED	Cleared IS-IS topology on the router.
MAXPATHCHANGE	Changed IP maximum parallel path.
NEWMETRIC	Changed link metric.
ATTACHFLAG	Changed Level 2 Attach bit.
ADMINDIST	Configured another administrative distance for the IS-IS instance on this router.
NEWADJ	Created a new adjacency to another router.
DELADJ	Deleted adjacency.
BACKUP	Installed backup route.
SEEDISPF	Seed incremental SPF.
NEXTHOP	Changed IP next-hop address.
NEWLSP0	New LSP 0 appeared in the topology.
LSPEXPIRED	Some LSP in the link-state database (LSDB) has expired.
LSPHEADER	Changed important LSP header fields.
TLVCODE	Type, length, and value (TLV) objects code mismatch, indicating that different TLV objects are included in the newest version of an LSP.
LINKTV	Changed Link TLV content.
PREFIXTLV	Changed Prefix TLV content.
AREAADDRTLV	Changed Area address TLV content.
IP ADDRTLV	Changed IP address TLV content.
TUNNEL	Changed RRR tunnel.

R3.3 Beta Draft—Cisco Confidential Information

The following is sample output from the **show isis spf-log** command with the **first** keyword specified:

```
RP/0/RP0/CPU0:router# show isis spf-log first 2
```

```

IISIS isp Level 1 IPv4 Unicast Route Calculation Log
      Time      Total Trig
Timestamp  Type (ms)  Nodes Count First Trigger LSP   Triggers
Mon Aug 16 2004
19:25:35.140 FSPF  1    1    1          12a5.00-00 NEWLSP0
19:25:35.646 FSPF  1    1    1          12a5.00-00 NEWADJ

IISIS isp Level 2 IPv4 Unicast Route Calculation Log
      Time      Total Trig
Timestamp  Type (ms)  Nodes Count First Trigger LSP   Triggers
Mon Aug 16 2004
19:25:35.139 FSPF  1    1    1          12a5.00-00 NEWLSP0
19:25:35.347 FSPF  1    1    2          12a5.00-00 NEWSADJ TLVCODE

```

Table 62 describes the significant fields shown in the output.

Table 62 *show isis spf-log first Field Descriptions*

Field	Description
Level	IS-IS level of the router.
Timestamp	Time at which the SPF calculation started.
Type	Type of route calculation. The possible types are incremental SPF (iSPF), full SPF (FSPF), or partial route calculation (PRC).
Time (ms)	Number of milliseconds taken to complete this SPF run. Elapsed time is wall clock time, not CPU time.
Nodes	Number of routers and pseudonodes (LANs) that make up the topology calculated in this SPF run.
Trig Count	Number of events that triggered this SPF run. When there is a topology change, often multiple link-state packets (LSPs) are received in a short time. Depending on the configuration of the spf-interval command, a router may wait for a fixed period of time before running a router calculation. This count denotes the number of triggering events that occurred while the router was waiting to run the calculation. For a full description of the triggering events, see Table 61.
First Trigger LSP	LSP ID stored by the router whenever a full SPF calculation is triggered by the arrival of a new LSP. The LSP ID can suggest the source of routing instability in an area. If multiple LSPs are causing an SPF run, only the LSP ID of the first received LSP is remembered.
Triggers	List of all reasons that triggered a full SPF calculation. For a list of possible triggers, see Table 61

The following is sample output from the **show isis spf-log** command with the **detail** keyword specified:

```
RP/0/RP0/CPU0:router# show isis spf-log detail
```

```

IISIS isp Level 1 IPv4 Unicast Route Calculation Log
      Time      Total Trig
Timestamp  Type (ms)  Nodes Count First Trigger LSP   Triggers
Mon Aug 16 2004
19:25:35.140 FSPF  1    1    1          12a5.00-00 NEWLSP0

```

R3.3 Beta Draft—Cisco Confidential Information

```

Delay:                    51ms (since first trigger)
SPT Calculation
  CPU Time:              0ms
  Real Time:             0ms
Prefix Updates
  CPU Time:              1ms
  Real Time:             1ms
New LSP Arrivals:        0
Next Wait Interval:      200ms

Results
Reach Unreach Total
Nodes:                    1      0      1
Prefixes (Items)
  Critical Priority:       0      0      0
  High Priority:          0      0      0
  Medium Priority         0      0      0
  Low Priority            0      0      0

  All Priorities         0      0      0
Prefixes (Routes)
  Critical Priority:       0      -      0
  High Priority:          0      -      0
  Medium Priority         0      -      0
  Low Priority            0      -      0

  All Priorities         0      -      0

```

Table 63 describes the significant fields shown in the output.

Table 63 *show isis spf-log detail Field Descriptions*

Field	Description
Level	IS-IS level of the router.
Timestamp	Time at which the SPF calculation started.
Type	Type of route calculation. The possible types are incremental SPF (iSPF), full SPF (FSPF), or partial route calculation (PRC).
Time (ms)	Number of milliseconds taken to complete this SPF run. Elapsed time is wall clock time, not CPU time.
Nodes	Number of routers and pseudonodes (LANs) that make up the topology calculated in this SPF run.
Trig Count	Number of events that triggered this SPF run. When there is a topology change, often multiple link-state packets (LSPs) are received in a short time. Depending on the configuration of the spf-interval command, a router may wait for a fixed period of time before running a router calculation. This count denotes the number of triggering events that occurred while the router was waiting to run the calculation. For a full description of the triggering events, see Table 61.
First Trigger LSP	LSP ID stored by the router whenever a full SPF calculation is triggered by the arrival of a new LSP. The LSP ID can suggest the source of routing instability in an area. If multiple LSPs are causing an SPF run, only the LSP ID of the first received LSP is remembered.
Triggers	List of all reasons that triggered a full SPF calculation. For a list of possible triggers, see Table 61

R3.3 Beta Draft – Cisco Confidential Information

Table 63 *show isis spf-log detail Field Descriptions (continued)*

Field	Description
Delay	Two different delays exist: 1. The delay between the time when the route calculation was first triggered and the time when it was run. 2. The delay between the end of the last route calculation and the start of this one. This is used to verify that the SPF-interval timers are working correctly, and is only reported for calculations after the first delay.
CPU Time	Two different CPU times exist: 1. CPU time (in milliseconds) taken to calculate the shortest path tree (SPT). 2. CPU time (in milliseconds) taken to perform the prefix updates.
Real Time	Two different real times exist: 1. Real time (in milliseconds) taken to calculate the shortest path tree (SPT). 2. Real time (in milliseconds) taken to perform the prefix updates.
New LSP Arrivals	Number of LSP arrivals since the start of this route calculation.
Next Wait Interval	Enforced delay until the next route calculation can be run, based on the spf-interval command configuration.
Reach	Number of reachable nodes or prefixes.
Unreach	Number of unreachable nodes or prefixes.
Total	Total number of nodes or prefixes at various priorities.

Related Commands

Command	Description
spf-interval	Sets IS-IS throttling of shortest path first (SPF) calculations.

R3.3 Beta Draft – Cisco Confidential Information

show isis statistics

To display Intermediate System-to-Intermediate System (IS-IS) traffic counters use the **show isis statistics** command in EXEC mode.

show isis [**instance** *instance-id*] **statistics** [*interface-type interface-number*]

Syntax Description		
instance <i>instance-id</i>	(Optional) Displays the IS-IS traffic statistics for the specified IS-IS instance only.	The <i>instance-id</i> argument is the instance identifier (alphanumeric) defined by the router isis command.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.	
<i>interface-number</i>	(Optional) Either a physical interface instance or a virtual interface instance as follows:	- Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults No instance ID specified displays IS-IS traffic statistics for all the IS-IS instances. IS-IS traffic statistics are displayed for all interfaces.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Release	Modification
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **show isis statistics** command displays IS-IS traffic counters for the specified interface or all traffic counters if no interface is specified.

Task ID

Task ID	Operations
isis	read

Examples

The following is sample output from the **show isis statistics** command that shows all traffic counters:

```
RP/0/RP0/CPU0:router# show isis statistics

ISIS isp statistics:
  ISIS statistics:
    Fast PSNP cache (hits/tries): 0/0
    LSP checksum errors received: 0
    IIH/LSP queue size: 400/1200
    IIH Dropped: 0
    LSP Dropped: 0
    SNP Dropped: 0
    IIH Max Queue size: 2
    UPD Max Queue size: 2
    Level-1:
      LSPs sourced (new/refresh): 8/0
      IPv4 Unicast
        SPF calculations          : 11
        iSPF calculations         : 0
        Partial Route Calculations: 0
    Level-2:
      LSPs sourced (new/refresh): 9/0
      IPv4 Unicast
        SPF calculations          : 11
        iSPF calculations         : 0
        Partial Route Calculations: 0
    Interface Loopback0:
      Level-1 LSPs (sent/rcvd)   : 0/0
      Level-1 CSNPs (sent/rcvd)  : 0/0
      Level-1 PSNPs (sent/rcvd)  : 0/0
      Level-2 LSPs (sent/rcvd)   : 0/0
      Level-2 CSNPs (sent/rcvd)  : 0/0
      Level-2 PSNPs (sent/rcvd)  : 0/0
    Interface POS4/1:
      PTP Hellos (sent/rcvd)     : 71/73
      LSP Retransmissions        : 8
      Level-1 LSPs (sent/rcvd)   : 8/5
      Level-1 CSNPs (sent/rcvd)  : 2/2
      Level-1 PSNPs (sent/rcvd)  : 2/3
      Level-2 LSPs (sent/rcvd)   : 8/7
      Level-2 CSNPs (sent/rcvd)  : 2/2
```

R3.3 Beta Draft—Cisco Confidential Information

```

Level-2 PSNPs (sent/rcvd) : 4/3
Interface POS0/5/0/1:
Level-1 Hellos (sent/rcvd): 199/68
Level-1 DR Elections      : 2
Level-1 LSPs (sent/rcvd)  : 6/3
Level-1 CSNPs (sent/rcvd) : 63/0
Level-1 PSNPs (sent/rcvd) : 0/16
Level-2 Hellos (sent/rcvd): 197/69
Level-2 DR Elections      : 2
Level-2 LSPs (sent/rcvd)  : 7/2
Level-2 CSNPs (sent/rcvd) : 66/0
Level-2 PSNPs (sent/rcvd) : 0/16

```

Table 64 describes the significant fields shown in the display.

Table 64 *show isis statistics Field Descriptions*

Field	Description
Fast PSNP cache (hits/tries):	Number of successful lookups (hits) along with the number of lookup attempts (tries). To save time or processing power when receiving multiple copies of the same LSP, IS-IS attempts to look up incoming LSPs to see if they have been received recently.
LSP checksum errors received:	Number of internal checksum errors received in LSPs.
IIH (LSP/SNP) dropped:	Number of hello, LSP, and SNP messages dropped.
IIH (UPD) Max Queue size:	Maximum number of queued packets.
LSPs sourced (new/refresh):	Number of LSPs this IS-IS instance has created or refreshed. More details on these LSPs can be found using the show isis lsp-log command.
SPF calculations:	Number of shortest path first (SPF) calculations. SPF calculations are performed only when the topology changes. They are not performed when external routes change. The interval at which SPF calculations are performed is configured using the spf-interval command.
iSPF calculations:	Number of incremental shortest path first (iSPF) calculations. iSPF calculations are performed only when ISPF has been configured in the isis address family configuration submode.
Partial Route Calculations:	Number of partial route calculations (PRCs). PRCs are processor intensive. Therefore, it may be useful to limit how often a PRC is done, especially on slower networking devices. Increasing the PRC interval reduces the processor load on the router, but potentially slows the rate of convergence. The interval at which PRC calculations are performed is configured using the spf-interval command.
Level-(1/2) (LSPs/CSNPs/PSNPs/Hellos) (sent/rcvd):	Number of LSPs, Complete Sequence Number Packets (CSNPs), Partial Sequence Number Packets (PSNPs), and hello packets sent or received on this interface.
PTP Hellos (sent/rcvd):	Point-to-point (PTP) hellos sent and received.

R3.3 Beta Draft – Cisco Confidential Information

Table 64 *show isis statistics Field Descriptions (continued)*

Field	Description
LSP Retransmissions:	Total number of retransmissions on each IS-IS LSP on a point-to-point interface. The LSP retransmission interval can be configured using the retransmit-throttle-interval command.
Level-(1,2) DR Elections:	Total number of Designated Intermediate System elections that have taken place. These counts are maintained on an individual level basis.

Related Commands

Command	Description
show isis spf-log	Displays how often and why the router has run a full SPF calculation.
spf-interval	Sets IS-IS throttling of shortest path first (SPF) calculations.

R3.3 Beta Draft—Cisco Confidential Information

show isis topology

To display a list of connected Intermediate System-to-Intermediate System (IS-IS) routers in all areas, use the **show isis topology** command in EXEC mode.

```
show isis [instance instance-id] [ipv4 | ipv6 | afi-all [unicast]] topology [summary | level {1 | 2}]
[systemid system-id] [detail]
```

Syntax Description		
instance <i>instance-id</i>	(Optional) Displays the IS-IS topology for the specified IS-IS instance only.	The <i>instance-id</i> argument is the instance identifier (alphanumeric) defined by the router isis command.
ipv4	(Optional) Specifies IP Version 4 address prefixes.	
ipv6	(Optional) Specifies IP Version 6 address prefixes.	
afi-all	(Optional) Specifies all address prefixes.	
unicast	(Optional) Specifies unicast address prefixes.	
summary	(Optional) Displays a brief list of the IS-IS topology.	
level {1 2}	(Optional) Displays the IS-IS link-state topology for Level 1 or Level 2 independently.	
systemid <i>system-id</i>	(Optional) Displays the information for the specified router only.	
details	(Optional) Displays detailed information on the IS-IS topology.	

Defaults No instance ID specified displays a list of connected routers in all areas for all the IS-IS instances. Both Level 1 and Level 2 is configured if no level is specified.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	The detail keyword was added.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show isis topology** command to verify the presence and connectivity among all routers in all areas.

R3.3 Beta Draft—Cisco Confidential Information

Task ID

Task ID Operations

isis	read

Examples

The following is sample output from the **show isis topology** command:

```
RP/0/RP0/CPU0:router# show isis topology
```

IS-IS isp paths to (Level-1) routers

System Id	Metric	Next-Hop	Interface	SNPA
ensoft-5	10	ensoft-5	PO0/4/0/1	*PtoP*
ensoft-5	10	ensoft-5	Gi0/5/0/0	0003.6cff.0680
ensoft-11	--			

IS-IS isp paths to (Level-2) routers

System Id	Metric	Next-Hop	Interface	SNPA
ensoft-5	10	ensoft-5	PO0/4/0/1	*PtoP*
ensoft-5	10	ensoft-5	Gi0/5/0/0	0003.6cff.0680
ensoft-11	--			

Table 65 describes the significant fields shown in the display.

Table 65 *show isis topology ipv4 unicast Field Descriptions*

Field	Description
System ID	Dynamic hostname of the system. The hostname is specified using the hostname command. If the dynamic hostname is not known or hostname dynamic disable command has been executed, the 6-octet system ID is used.
Metric	Metric assigned to the link and used to calculate the cost from each router using the links in the network to other destinations. Range is 1 to 16777214. Default is 1 to 63 for narrow metric and 1 to 16777214 for wide metric. 0 is set internally if no metric has been specified by the user.
Next-Hop	Address of the next hop.
Interface	Interface used to reach the neighbor.
SNPA	Data-link address (also known as the Subnetwork Point of Attachment [SNPA]) of the neighbor.

The following is sample output from the **show isis topology** command with the **summary** keyword specified:

```
RP/0/RP0/CPU0:router# show isis topology summary
```

IS-IS 10 IS Topology Summary IPv4 Unicast

	L1			L2		
	Reach	UnReach	Total	Reach	UnReach	Total
Router nodes:	1	1	2	1	1	2
Pseudo nodes:	0	0	0	0	0	0
Total nodes:	1	1	2	1	1	2

Table 66 describes the significant fields shown in the display.

R3.3 Beta Draft—Cisco Confidential Information**Table 66** *show isis topology summary Field Descriptions*

Field	Description
L1/L2	IS-IS level of the router.
Reach	Number of router nodes or pseudonodes that are reachable.
UnReach	Number of router nodes or pseudonodes that are unreachable.
Total	Total number of reachable and unreachable nodes.

R3.3 Beta Draft—Cisco Confidential Information

show protocols (IS-IS)

To group a number of protocol show commands according to the specified address family, use the **show protocols** command in interface configuration mode.

show protocols [**afi-all** | **ipv4** | **ipv6**] [**all** | *protocol*]

Syntax Description	
afi-all	(Optional) Specifies all address families.
ipv4	(Optional) Specifies an IPv4 address family.
ipv6	(Optional) Specifies an IPv6 address family.
all	(Optional) Specifies all protocols for a given address family.
<i>protocol</i>	(Optional) Specifies a routing protocol. For the IPv4 address family, the options are: bgp isis ospf For the IPv6 address family, the options are bgp isis ospfv3

Defaults If no address family is specified, the default is IPv4.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The afi-all keyword was added.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If IPv6 is enabled on an IS-IS instance, the instance is displayed in the **show protocols ipv6** command output. IPv4 IS-IS instances are displayed in the **show protocols ipv4** command output.

When using the **show protocols** command with the **ipv6** or **ipv4** keyword, you get all routing instances in that particular address family—not only IS-IS instances.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	isis	read
	rib	read

Examples

The following example shows the output for the **show protocols** command using the **ipv6** keyword:

```
RP/0/RP0/CPU0:router# show protocols ipv6
```

```
IS-IS Router: uut
System Id: 0000.0000.12a8
IS Levels: level-1-2
Manual area address(es):
  49.1515.1515
Routing for area address(es):
  49.1515.1515
Non-stop forwarding: Disabled
Most recent startup mode: Cold Restart
Topologies supported by IS-IS:
  IPv4 Unicast
    Level-1
      Metric style (generate/accept): Narrow/Narrow
      ISPF status: Disabled
    Level-2
      Metric style (generate/accept): Narrow/Narrow
      ISPF status: Disabled
      Redistributing:
        static
      Distance: 115
  IPv6 Unicast
    Level-1
      ISPF status: Disabled
    Level-2
      ISPF status: Disabled
      No protocols redistributed
      Distance: 45
Interfaces supported by IS-IS:
  POS 0/6/0/0 is running actively (active in configuration)
```

Table 67 describes the significant fields shown in the display.

Table 67 *show protocols ipv6 Field Descriptions*

Field	Description
System ID	Dynamic hostname of the system. The hostname is specified using the hostname command. If the dynamic hostname is not known or hostname dynamic disable command has been executed, the 6-octet system ID is used.
IS Levels	IS-IS level of the router.
Manual area address(es)	Area addresses configured manually on the originating router.
Routing for area address(es)	Area addresses for which this router provides the routing.
Non-stop forwarding	Status and name of NSF.
Most recent startup mode	Mode in which the most recent startup was performed.

R3.3 Beta Draft – Cisco Confidential Information

Table 67 *show protocols ipv6 Field Descriptions (continued)*

Field	Description
Topologies supported by IS-IS	Address and subaddress family IS-IS are configured.
Metric style	Type, length, and value (TLV) objects accepted by IS-IS. To configure this value, see the metric-style narrow , metric-style transition , or metric-style wide command.
ISPF status	State of iSPF configuration for this IS-IS instance. Four states exist: • Disabled if iSPF has not been configured but is awaiting a full SPF to compile the topology for use by the iSPF algorithm. • Dormant if iSPF has been configured but is awaiting initial convergence before initializing. • Awake if iSPF has been configured but is awaiting a full SPF to compile the topology for use by the iSPF algorithm. • Active if IS-IS is ready to consider using the iSPF algorithm whenever a new route calculation needs to be run.
Redistributing	IS-IS is configured to redistribute IP static routes into Level 1 or Level 2. The redistribute command is used to configure redistribution.
Distance	Administrative distance.
Interfaces supported by IS-IS	Interfaces and their states currently supported by IS-IS.

The following example shows how to disable the IPv6 address family, then no output is shown for IS-IS IPv6 instances from the **show protocols ipv6** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router isis uut
RP/0/RP0/CPU0:router(config-isis)# no address-family ipv6 unicast
RP/0/RP0/CPU0:router(config-isis)# commit

RP/0/RP0/CPU0:router# show protocols ipv6
```

Related Commands

Command	Description
metric-style narrow	Configures the IS-IS software to generate and accept old-style type, length, and value (TLV) objects.
metric-style transition	Configures the IS-IS software to generate and accept both old-style and new-style type length, and value (TLV) objects.
metric-style wide	Configures the IS-IS software to generate and accept only new-style type, length, and value (TLV) objects.
redistribute (IS-IS)	Redistributes routes from one IS-IS instance into another instance.

R3.3 Beta Draft—Cisco Confidential Information

shutdown (IS-IS)

To disable the Intermediate System-to-Intermediate System (IS-IS) protocol on a particular interface, use the **shutdown** command in interface configuration mode. To re-enable the IS-IS protocol, use the **no** form of this command.

shutdown

no shutdown

Syntax Description	This command has no arguments or keywords.

Defaults	IS-IS protocol is enabled.

Command Modes	Interface configuration

Command History	Release	Modification
	Release 2.0	This command was introduced.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	isis	read, write

Examples	The following example disables the IS-IS protocol on Packet-over-SONET (POS) interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# interface POS0/1/0/1
RP/0/RP0/CPU0:router(config-isis-if)# shutdown
```

R3.3 Beta Draft—Cisco Confidential Information

single-topology

To configure the link topology for IP Version 4 (IPv4) when IP Version 6 (IPv6) is configured, use the **single-topology** command in router address family configuration mode. To remove the **single-topology** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

single-topology

no single-topology

Syntax Description

This command has no arguments or keywords.

Defaults

Performs in multitopology mode in which independent topologies for IPv4 and IPv6 are running in a single area or domain.

Command Modes

Router address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **single-topology** command to allow Intermediate System-to-Intermediate System (IS-IS) for IPv6 to be configured on interfaces along with an IPv4 network protocol. All interfaces must be configured with the identical set of network protocols, and all routers in the IS-IS area (for Level 1 routing) or the domain (for Level 2 routing) must support the identical set of network layer protocols on all interfaces.

When single-topology support for IPv6 is being used, only old-style type, length, and value (TLV) objects may be used and a single shortest path (SPF) individual level is used to compute IPv4 (if configured) and IPv6 routes. The use of a single SPF means that both IPv4 IS-IS and IPv6 IS-IS routing protocols must share a network topology.

To allow link information to be shared between IPv4 and IPv6, you must configure the **single-topology** command for an address family. In single-topology IPv6 mode, the configured metric is always the same for both IPv4 and IPv6.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	isis	read, write

Examples

The following example shows how to enable single-topology mode for IPv6:

```
RP/0/RP0/CPU0:router(config)# router isis isp  
RP/0/RP0/CPU0:router(config-isis)# net 49.0000.0000.0001.00  
RP/0/RP0/CPU0:router(config-isis)# address-family ipv6 unicast  
RP/0/RP0/CPU0:router(config-isis-af)# single-topology
```

R3.3 Beta Draft—Cisco Confidential Information

spf-interval

To customize IS-IS throttling of shortest path first (SPF) calculations, use the **spf-interval** command in router address family configuration mode. To restore default values, use the **no** form of this command.

spf-interval {[**initial-wait** *initial* | **secondary-wait** *secondary* | **maximum-wait** *maximum*]
...}[**level** {**1** | **2**}]

no spf-interval

Syntax Description

initial-wait <i>initial</i>	Initial SPF calculation delay (in milliseconds) after a topology change. Range is 0 to 120000 milliseconds.
secondary-wait <i>secondary</i>	Hold time between the first and second SPF calculations (in milliseconds). Range is 1 to 120000 milliseconds.
maximum-wait <i>maximum</i>	Maximum interval (in milliseconds) between two consecutive SPF calculations. Range is 1 to 120000 milliseconds.
level { 1 2 }	(Optional) Enables the SPF interval configuration for Level 1 or Level 2 independently.

Defaults

initial-wait *initial*: 50 milliseconds
secondary-wait *secondary*: 200 milliseconds
maximum-wait *maximum*: 5000 milliseconds

Command Modes

Router address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	The initial-wait <i>initial</i> , secondary-wait <i>secondary</i> , and maximum-wait <i>maximum</i> keywords and arguments were added.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

SPF calculations are performed only when the topology changes. They are not performed when external routes change.

Use the **spf-interval** command to control how often the software can perform the SPF calculation. The SPF calculation is processor intensive. Therefore, it may be useful to limit how often this calculation is done, especially when the area is large and the topology changes often. Increasing the SPF interval reduces the processor load of the router, but potentially slows the rate of convergence.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	isis	read, write

Examples

The following example shows how to set the initial SPF calculation delay to 10 milliseconds and the maximum interval between two consecutive SPF calculations to 5000 milliseconds:

```
RP/0/RP0/CPU0:router(config)# router isis isp  
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast  
RP/0/RP0/CPU0:router(config-isis-af)# spf-interval initial-wait 10 maximum-wait 5000
```

R3.3 Beta Draft—Cisco Confidential Information

summary-prefix (IS-IS)

To create aggregate addresses for the Intermediate System-to-Intermediate System (IS-IS) protocol, use the **summary-prefix** command in router address family configuration mode. To restore the default behavior, use the **no** form of this command.

summary-prefix [*address/prefix-length* | *ipv6-prefix/prefix-length*] [**level** {**1** | **2**}]

no summary-prefix

Syntax Description

<i>address</i>	(Optional) Summary address designated for a range of IPv4 addresses. The <i>address</i> argument must be in four-part, dotted-decimal notation.
<i>/prefix-length</i>	(Optional) Length of the IPv4 or IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value.
<i>ipv6-prefix</i>	(Optional) Summary prefix designated for a range of IPv6 prefixes. The <i>ipv6-prefix</i> argument must be in the form documented in RFC 2373, in which the address is specified in hexadecimal using 16-bit values between colons.
level { 1 2 }	(Optional) Redistributes routes into Level 1 or Level 2 and summarizes them with the configured address and mask value.

Defaults

All redistributed routes are advertised individually.
Both Level 1 and Level 2 are configured if no level is specified.

Command Modes

Router address family configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Multiple groups of addresses can be summarized for a given level. Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the more-specific routes. Use the **summary-prefix** command to help reduce the size of the routing table.

R3.3 Beta Draft—Cisco Confidential Information

This command also reduces the size of the link-state packets (LSPs) and thus the link-state database. It also helps ensure stability, because a summary advertisement depends on many more specific routes. If one more-specific route flaps, in most cases, this flap does not cause a flap of the summary advertisement.

The drawback of summary addresses is that other routes might have less information to calculate the most optimal routing table for all individual destinations.

**Note**

When IS-IS advertises a summary prefix, it automatically inserts the summary prefix into the IP routing table but labels it as a “discard” route entry. Any packet that matches the entry is discarded to prevent routing loops. When IS-IS stops advertising the summary prefix, the routing table entry is removed.

Task ID**Task ID****Operations**

isis

read, write

Examples

The following example shows how to redistribute Open Shortest Path First (OSPF) routes into IS-IS. In the OSPF routing table, IPv6 routes exist for 3ffe:f000:0001:0000::/64, 3ffe:f000:0002:0000::/64, 3ffe:f000:0003:0000::/64, and so on. This example shows only 3ffe:f000::/24 advertised into IPv6 IS-IS Level 2.

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# address-family ipv6 unicast
RP/0/RP0/CPU0:router(config-isis-af)# redistribute ospf 2 level-2
RP/0/RP0/CPU0:router(config-isis-af)# summary-prefix 3ffe:f000::/24 level-2
```

■ suppressed

R3.3 Beta Draft—Cisco Confidential Information

suppressed

To allow an IS-IS interface to participate in forming adjacencies without advertising connected prefixes in the system link-state packets (LSPs), use the **suppressed** command in interface configuration mode. To enable advertising connected prefixes, use the **no** form of this command.

suppressed

no suppressed

Syntax Description This command has no arguments or keywords.

Defaults Interface is active.

Command Modes Interface configuration

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **suppressed** command to reduce the number of routes that IS-IS has to maintain, improving convergence times after an isolated failure. Improvement is noticeable if the command is used widely throughout the network. Other routers in the domain do not install routes to the affected connected prefixes.

Task ID	Task ID	Operations
	isis	read, write

Examples The following example shows how to disable the advertisement of connected prefixes on Packet-over-SONET (POS) interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# router isis isp
RP/0/RP0/CPU0:router(config-isis)# interface POS0/1/0/1
RP/0/RP0/CPU0:router(config-isis-if)# suppressed
```

R3.3 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	passive (IS-IS)	Suppresses S-IS packets on an interface.

 suppressed

R3.3 Beta Draft – Cisco Confidential Information

OSPF Commands on Cisco IOS XR Software

Beta Draft Highly Confidential Information

This chapter describes the commands used to configure and monitor the Open Shortest Path First (OSPF) routing protocol.

For detailed information about OSPF concepts, configuration tasks, and examples, see the *Implementing OSPF on Cisco IOS XR Software* configuration guide.

R3.3 Beta Draft—Cisco Confidential Information

address-family (OSPF)

To enter address family configuration mode for Open Shortest Path First (OSPF), use the **address-family** command in the router configuration mode. To disable address family configuration mode, use the **no** form of this command.

address-family ipv4 [unicast]

no address-family ipv4 [unicast]

Syntax Description	ipv4	Specifies IP Version 4 (IPv4) address prefixes.
	unicast	(Optional) Specifies unicast address prefixes.

Defaults The default is unicast if an address-family is not specified.

Command Modes Router configuration
VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was added under the VRF configuration mode. This command was added under the VRF configuration mode.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

OSPF version 2 automatically provides routing services for IPv4 unicast topologies, so this command is redundant.

Task ID	Task ID	Operations
	ospf	read, write

Examples The following example shows how to configure the OSPF router process with IPv4 unicast address prefixes:

```
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# address-family ipv4 unicast
```

R3.3 Beta Draft—Cisco Confidential Information

area (OSPF)

To configure an Open Shortest Path First (OSPF) area, use the **area** command in router configuration mode. To terminate an OSPF area, use the **no** form of this command.

area *area-id*

no area *area-id*

Syntax Description

<i>area-id</i>	Identifier of an OSPF area. The <i>area-id</i> argument can be specified as either a decimal value or an IP address.

Defaults

No OSPF area is defined.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **area** command to explicitly configure an area. Commands configured under the area configuration mode (such as the **interface** [OSPF] and **authentication** commands), are automatically bound to that area.

To modify or remove the area, the *area-id* argument format must be the same as the format used when creating the area. Otherwise, even if the actual 32-bit value matches, the area is not matched. For example, if you create an area with an *area-id* of 10 it would not match an *area-id* of 0.0.0.10.

**Note**

To remove the specified area from the router configuration, use the **no area** *area-id* command. The **no area** *area-id* command removes the area and all area options, such as **authentication**, **default-cost**, **nssa**, **range**, **stub**, **virtual-link**, and **interface**

Task ID

Task ID	Operations
ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure area 0 and Packet-over-SONET/SDH (POS) interface 0/2/0/0. POS interface 0/2/0/0 is bound to area 0 automatically.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/2/0/0
```

R3.3 Beta Draft—Cisco Confidential Information

authentication (OSPF)

To enable plain text, Message Digest 5 (MD5) authentication, or null authentication for an Open Shortest Path First (OSPF) interface, use the **authentication** command in the appropriate mode. To remove such authentication, use the **no** form of this command.

authentication [**message-digest** | **null**]

no authentication

Syntax Description

message-digest	(Optional) Specifies that MD5 is used.
null	(Optional) Specifies that no authentication is used. Useful for overriding password or MD5 authentication if configured for an area.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the authentication parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the authentication parameter specified for the process.

If this command is not specified at any level, then the interface does not use authentication.

If no keyword is specified, plain text authentication is used.

Command Modes

Interface configuration
Area configuration
Router configuration
Virtual-link configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **authentication** command to specify an authentication type for the interface, which overrides the authentication specified for the area to which this interface belongs. If this command is not included in the configuration file, the authentication configured in the area to which the interface belongs is assumed (as specified by the area **authentication** command).

The authentication type and password must be the same for all OSPF interfaces that are to communicate with each other through OSPF. If you specified plain text authentication, use the **authentication-key** command to specify the plain text password.

R3.3 Beta Draft – Cisco Confidential Information

If you enable MD5 authentication with the **message-digest** keyword, you must configure a key with the **message-digest-key** interface command.

Task ID	Task ID	Operations
	ospf	read, write

Examples The following example shows how to set authentication for areas 0 and 1 of OSPF routing process 201. Authentication keys are also provided.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 201
RP/0/RP0/CPU0:router(config-ospf)# router-id 10.1.1.1
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# authentication
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-ospf-ar-if)# authentication-key mykey
RP/0/RP0/CPU0:router(config-ospf-ar-if)# exit
RP/0/RP0/CPU0:router(config-ospf)# area 1
RP/0/RP0/CPU0:router(config-ospf-ar)# authentication
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/1/0/0
RP/0/RP0/CPU0:router(config-ospf-ar-if)# authentication-key mykey1
```

Related Commands	Command	Description
	authentication-key (OSPF)	Assigns a password to be used by neighboring routers that are using the simple password authentication of OSPF.
	message-digest-key	Enables OSPF MD5 authentication.

R3.3 Beta Draft—Cisco Confidential Information

authentication-key (OSPF)

To assign a password to be used by neighboring routers that are using the Open Shortest Path First (OSPF) simple password authentication, use the **authentication-key** command in the appropriate mode. To remove a previously assigned OSPF password, use the **no** form of this command.

authentication-key [**clear** | **encrypted**] *password*

no authentication-key

Syntax Description

clear	(Optional) Specifies that the key be clear text.
encrypted	(Optional) Specifies that the key be encrypted using a two-way algorithm.
<i>password</i>	Any contiguous string of characters up to 8 bytes in length that can be entered from the keyboard.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the OSPF password parameter specified by the area.
If this command is not specified in area configuration mode, then the interface adopts the OSPF password parameter specified for the process.
If this command is not specified at any level, then no password is specified.
Clear is the default if the **clear** or **encrypted** keyword is not specified.

Command Modes

Interface configuration
Area configuration
Router configuration
Virtual-link configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The 0 and 7 keywords were changed to clear and encrypted .
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The password created by this command is used as a “key” that is inserted directly into the OSPF header when the Cisco IOS XR software originates routing protocol packets. A separate password can be assigned to each network on an individual interface basis. All neighboring routers on the same network must have the same password to be able to exchange OSPF information.

R3.3 Beta Draft – Cisco Confidential Information

The **authentication-key** command must be used with the **authentication** command. If the **authentication** command is not configured, the password provided by the **authentication-key** command is ignored and no authentication is adopted by the OSPF interface.



Note

The **authentication-key** command cannot be used with the **authentication** command when the **message-digest** or **null** keyword is configured.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to enable the authentication key with the string yourpass:

```
RP/0/RP0/CPU0:router# configure  
RP/0/RP0/CPU0:router(config)# router ospf 201  
RP/0/RP0/CPU0:router(config-ospf)# authentication-key yourpass
```

Related Commands

Command	Description
authentication (OSPF)	Specifies authentication type.

R3.3 Beta Draft—Cisco Confidential Information**auto-cost (OSPF)**

To control how the Open Shortest Path First (OSPF) protocol calculates default metrics for the interface, use the **auto-cost** command in router configuration mode. To revert to the default reference bandwidth, use the **no** form of this command.

auto-cost { **reference-bandwidth** *mbps* | **disable** }

no auto-cost [**reference-bandwidth** | **disable**]

Syntax Description

reference-bandwidth <i>mbps</i>	Specifies a rate in Mbps (bandwidth). Range is 1 to 4294967.
disable	Assigns a cost based on interface type.

Defaults

mbps: 100 Mbps

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

By default OSPF calculates the OSPF metric for an interface according to the bandwidth of the interface.

The OSPF metric is calculated as the *mbps* value divided by bandwidth, with *mbps* equal to 10^8 by default.

If you have multiple links with high bandwidth (such as OC-192), you might want to use a larger number to differentiate the cost on those links. That is, the metric calculated using the default *mbps* value is the same for all high-bandwidth links.

Recommended usage of cost configuration for all OSPF configured interfaces is to be consistent: Either explicitly configure (by using the **cost** command) or choose default (by using the **auto-cost** command).

The value set by the **cost** command overrides the cost resulting from the **auto-cost** command.

**Note**

The configuration setting of this command must be duplicated on every OSPF router in the autonomous system.

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows how to set the reference value for the auto cost calculation to 1000 Mbps:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# auto-cost reference-bandwidth 1000
```

Related Commands	Command	Description
	cost (OSPF)	Explicitly specifies the cost of sending a packet on an interface.

R3.3 Beta Draft—Cisco Confidential Information

capability opaque

To control opaque link-state advertisement (LSA) support capability of the Open Shortest Path First (OSPF) protocol, use the **capability opaque** command in router configuration mode. To prevent Multiprotocol Label Switching traffic engineering (MPLS TE) topology information flooded to the network through opaque LSAs, use the **disable** form of this command.

capability opaque [**disable**]

no capability opaque [**disable**]

Syntax Description	enable	(Optional) Enables opaque LSA support capability.
	disable	(Optional) Disables opaque LSA support capability.

Defaults Opaque LSAs are allowed.

Command Modes Router configuration
VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The enable keyword was removed.
	Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Control opaque LSA support capability must be enabled for OSPF to support MPLS TE. The MPLS TE topology information is flooded to the network through opaque LSAs of OSPF.

Task ID	Task ID	Operations
	ospf	read, write

Examples The following example shows how to prevent OSPF from supporting opaque services:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# capability opaque disable
```

R3.3 Beta Draft—Cisco Confidential Information

clear ospf process

To reset an Open Shortest Path First (OSPF) router process without stopping and restarting it, use the **clear ospf process** command in EXEC mode.

clear ospf [*process-name* [**vrf** [*vrf-name* | **all**]]] **process**

Syntax Description

<i>process-name</i>	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the router ospf command. If this argument is included, only the specified routing process is affected. Otherwise, all OSPF processes are reset.
vrf	(Optional) An OSPF VPN Routing and Forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of the OSPF VRF instance to be reset.
all	(Optional) Resets all OSPF VRF instances.

Defaults

No default behavior or value

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	The vrf keyword was added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When the OSPF router process is reset, OSPF releases all resources allocated, cleans up the internal database, and shuts down and restarts all interfaces that belong to the process.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to reset all OSPF processes:

```
RP/0/RP0/CPU0:router# clear ospf process
```

R3.3 Beta Draft—Cisco Confidential Information

The following example shows how to reset the OSPF process 1:

```
RP/0/RP0/CPU0:router# clear ospf 1 process
```

Related Commands	Command	Description
	router ospf	Configures an OSPF routing process.

R3.3 Beta Draft—Cisco Confidential Information

clear ospf redistribution

To clear all routes redistributed from other protocols out of the Open Shortest Path First (OSPF) routing table, use the **clear ospf redistribution** command in EXEC mode.

clear ospf [*process-name* [**vrf** [*vrf-name* | **all**]]] **redistribution**

Syntax Description

<i>process-name</i>	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the router ospf command. If this argument is included, only the specified routing process is affected. Otherwise, all OSPF routes are cleared.
vrf	(Optional) OSPF VPN Routing and Forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of the OSPF VRF instance to be reset.
all	(Optional) Resets all OSPF VRF instances.

Defaults

No default behavior or value

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	The vrf keyword was added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **clear ospf redistribution** command to cause the routing table to be read again. OSPF regenerates and sends Type 5 and Type 7 link-state advertisements (LSAs) to its neighbors. If an unexpected route has appeared in the OSPF redistribution, using this command corrects the issue.



Note

Use of this command can cause a significant number of LSAs to flood the network. We recommend that you use this command with caution.

Task ID

Task ID	Operations
ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to clear all redistributed routes across all processes from other protocols:

```
RP/0/RP0/CPU0:router# clear ospf redistribution
```

R3.3 Beta Draft—Cisco Confidential Information

clear ospf routes

To clear all Open Shortest Path First (OSPF) routes from the OSPF routing table, use the **clear ospf routes** command in EXEC mode.

clear ospf [*process-name* [**vrf** [*vrf-name* | **all**]]] **routes**

Syntax Description

<i>process-name</i>	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the router ospf command. If this argument is included, only the specified routing process is affected. Otherwise, all OSPF routes are cleared.
vrf	(Optional) OSPF VPN Routing and Forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of the OSPF VRF instance to be reset.
all	(Optional) Resets all OSPF VRF instances.

Defaults

No default behavior or value

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The topology keyword was replaced with the routes keyword.
Release 3.3	The vrf keyword was added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to clear all OSPF routes from the OSPF routing table and recompute valid routes. When the OSPF routing table is cleared, OSPF routes in the global routing table are also recalculated.

```
RP/0/RP0/CPU0:router# clear ospf routes
```


R3.3 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
router ospf	Configures an OSPF routing process.

R3.3 Beta Draft—Cisco Confidential Information

clear ospf statistics

To clear the Open Shortest Path First (OSPF) statistics of neighbor state transitions, use the **clear ospf statistics** command in EXEC mode.

```
clear ospf [process-name [vrf [vrf-name | all]]] statistics [neighbor [interface-type
interface-instance] [ip-address]]
```

Syntax Description

<i>process-name</i>	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the router ospf command. If this argument is included, only the specified routing process is affected. Otherwise, all OSPF statistics of neighbor state transitions are cleared.
vrf	(Optional) OSPF VPN Routing and Forwarding (VRF) instance.
<i>vrf-name</i>	(Optional) Name of the OSPF VRF instance to be reset.
all	(Optional) Resets all OSPF VRF instances.
neighbor	(Optional) Clears the state transition counters of the specified neighbor only.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
<i>ip-address</i>	(Optional) IP address of a specified neighbor for whom you want to clear the state transition counter.

Defaults

No default behavior or value

Command Modes

EXEC

R3.3 Beta Draft—Cisco Confidential Information

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	The vrf keyword was added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **clear ospf statistics** command to reset OSPF counters. Reset is useful to detect changes in counter values.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to reset the OSPF transition state counters for all neighbors on Packet-over-SONET/SDH (POS) interface 0/2/0/0:

```
RP/0/RP0/CPU0:router# clear ospf statistics neighbor POS 0/2/0/0
```

Related Commands

Command	Description
router ospf	Configures an OSPF routing process.

R3.3 Beta Draft—Cisco Confidential Information**cost (OSPF)**

To explicitly specify the cost of sending a packet on an Open Shortest Path First (OSPF) interface, use the **cost** command in the appropriate mode. To remove the cost, use the **no** form of this command.

cost *cost*

no cost

Syntax Description

<i>cost</i>	Unsigned integer value expressed as the link-state metric. Range is 1 to 65535.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the cost parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the cost parameter specified for the process.

If this command is not specified at any level, then the cost is calculated by the **auto-cost** command.

Command Modes

Interface configuration
Area configuration
Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The link-state metric is advertised as the link cost in the router link advertisement. Cisco IOS XR software does not support type of service (ToS), so you can assign only one cost for each interface.

In general, the path cost is calculated using the following formula:

$10^8 / \text{bandwidth}$ (the default auto cost is set to 100 Mbps)

This calculation is the default reference bandwidth used by the auto-costing calculation which establishes the interface auto-cost. The **auto-cost** command can set this reference bandwidth to some other value. The **cost** command is used to override the auto-costing calculated default value for interfaces.

R3.3 Beta Draft—Cisco Confidential Information

Using this formula, the default path cost is 1 for any interface that has a link bandwidth of 100 Mbps or higher. If this value does not suit the network, configure the reference bandwidth for auto calculating costs based on the link bandwidth.

The value set by the **cost** command overrides the cost resulting from the **auto-cost (OSPF)** command.

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows how to set the cost value to 65 for Packet-over-SONET/SDH (POS) interface 0/1/0/1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-ospf-ar-if)# cost 65
```

Related Commands	Command	Description
	auto-cost (OSPF)	Controls how the OSPF protocol calculates default metrics for the interface.

R3.3 Beta Draft—Cisco Confidential Information

database-filter all out (OSPF)

To filter outgoing link-state advertisements (LSAs) to an Open Shortest Path First (OSPF) interface, use the **database-filter all out** command in interface configuration mode. To restore the forwarding of LSAs to the interface, use the **disable** form of the command.

database-filter all out [**disable** | **enable**]

Syntax Description	disable	(Optional) Disables filtering.
	enable	(Optional) Enables filtering.

Defaults The database filter is disabled.

Command Modes Interface configuration
Area configuration
Router configuration
VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **database-file all out** command to perform the same function that the **neighbor database-filter all out** command performs on a neighbor basis.

Task ID	Task ID	Operations
	ospf	read, write

Examples The following example shows how to prevent flooding of OSPF LSAs to broadcast, nonbroadcast, and point-to-point networks reachable through Packet-over-SONET/SDH (POS) interface 0/1/0/1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-ospf-ar-if)# database-filter all out
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	<code>neighbor database-filter all out</code>	Filters outgoing LSAs to an OSPF interface.

R3.3 Beta Draft—Cisco Confidential Information

dead-interval (OSPF)

To set the interval after which a neighbor is declared dead when no hello packets are observed, use the **dead-interval** command in the appropriate configuration mode. To return to the default time, use the **no** form of this command.

dead-interval *seconds*

no dead-interval

Syntax Description

<i>seconds</i>	Integer that specifies the interval (in seconds). Range is 1 to 65535. The value must be the same for all nodes on the network.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the dead interval parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the dead interval parameter specified for the process.

If this command is not specified at any level, then the dead interval is four times the interval set by the **hello-interval** (OSPF) command.

Command Modes

Interface configuration
Area configuration
Router configuration
Virtual-link configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The dead interval value must be the same for all routers and access servers on a specific network.

If the hello interval is configured, the dead interval value must be larger than the hello interval value. The dead interval value is usually configured four times larger than the hello interval value.

Task ID

Task ID	Operations
ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to set the OSPF dead interval to 40 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-ospf-ar-if)# dead-interval 40
```

Related Commands

Command	Description
hello-interval (OSPF)	Specifies the interval between hello packets that the Cisco IOS XR software sends on the interface.

R3.3 Beta Draft—Cisco Confidential Information

default-cost (OSPF)

To specify a cost for the default summary route sent into a stub area or not-so-stubby area (NSSA), use the **default-cost** command in area configuration mode. To remove the assigned default route cost, use the **no** form of this command.

default-cost *cost*

no default-cost *cost*

Syntax Description	<i>cost</i>	Cost for the default summary route used for a stub or NSSA area. The acceptable value is a 24-bit number.

Defaults	<i>cost</i> : 1

Command Modes	Area configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **default-cost** command only on an Area Border Router (ABR) attached to a stub or an NSSA area.

In all routers and access servers attached to the stub area, the area should be configured as a stub area using the **stub** command in the area submode. Use the **default-cost** command only on an ABR attached to the stub area. The **default-cost** command provides the metric for the summary default route generated by the ABR into the stub area

Task ID.	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to assign a default cost of 20 to a stub area (the Packet-over-SONET/SDH (POS) interface 0/4/0/3 is also configured in the stub area):

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 201
RP/0/RP0/CPU0:router(config-ospf)# area 10.15.0.0
RP/0/RP0/CPU0:router(config-ospf-ar)# stub
RP/0/RP0/CPU0:router(config-ospf-ar)# default-cost 20
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/4/0/3
```

Related Commands

Command	Description
stub (OSPF)	Defines an area as a stub area.

R3.3 Beta Draft—Cisco Confidential Information**default-information originate (OSPF)**

To generate a default external route into an Open Shortest Path First (OSPF) routing domain, use the **default-information originate** command in router configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**always**] [**metric** *metric-value*] [**metric-type** *type-value*]
 [**route-policy** *policy-name*]

no default-information originate

Syntax Description	always	(Optional) Always advertises the default route regardless of whether the routing table has a default route.
	metric <i>metric-value</i>	(Optional) Specifies the metric used for generating the default route. If you omit a value and do not specify a value using the default-metric command, the default metric value is 10. Range is 1 to 16777214.
	metric-type <i>type-value</i>	(Optional) Specifies the external link type associated with the default route advertised into the OSPF routing domain. It can be one of the following values: • 1—Type 1 external route • 2—Type 2 external route
	route-policy <i>policy-name</i>	(Optional) Specifies that a routing policy be used and the routing policy name.

Defaults	When you do not use this command in router configuration mode, no default external route is generated into an OSPF routing domain.
	<i>metric-value</i> : 10 <i>type-value</i> : 2

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was added under the VRF configuration mode. The policy keyword was changed to route-policy .

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Whenever you use the **redistribute** or **default-information originate** command to redistribute routes into an OSPF routing domain, the software automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the OSPF routing domain. The software still must have a default route for itself before it generates one, except when you have specified the **always** keyword.

For information about routing policies, see the *Routing Policy Commands on Cisco IOS XR Software* module of *Cisco IOS XR Routing Command Reference*.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to specify a metric of 100 for the default route redistributed into the OSPF routing domain and an external metric type of Type 1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 109
RP/0/RP0/CPU0:router(config-ospf)# redistribute igmp 108 metric 100
RP/0/RP0/CPU0:router(config-ospf)# default-information originate metric 100 metric-type 1
```

Related Commands

Command	Description
redistribute (OSPF)	Redistributes routes from one routing domain into a specified OSPF process.

R3.3 Beta Draft—Cisco Confidential Information

default-metric (OSPF)

To set default metric values for routes redistributed from another protocol into the Open Shortest Path First (OSPF) protocol, use the **default-metric** command in router configuration mode. To return to the default state, use the **no** form of this command.

- default-metric** *value*
- no default-metric** *value*

Syntax Description	<i>value</i>	Default metric value appropriate for the specified routing protocol. Range is 1 to 16777214.

Defaults	Built-in, automatic metric translations, as appropriate for each routing protocol. Current metrics are displayed in the show ospf summary-prefix command output. Note that this output is only displayed if there are routes currently redistributed from protocols.

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the default-metric command with the redistribute command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, use a default metric to provide a reasonable substitute and enable the redistribution to proceed.

Task ID	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to advertise Intermediate System-to-Intermediate System (IS-IS) protocol-derived routes into OSPF and assign a metric of 10:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf# default-metric 10
RP/0/RP0/CPU0:router(config-ospf)# redistribute isis 15
```

Related Commands

Command	Description
redistribute (OSPF)	Redistributes routes from one routing domain into a specified OSPF process.
show ospf summary-prefix	Displays OSPF aggregated summary address information.

R3.3 Beta Draft—Cisco Confidential Information

demand-circuit (OSPF)

To configure the Open Shortest Path First (OSPF) protocol to treat the interface as an OSPF demand circuit, use the **demand-circuit** command in the appropriate mode. To remove the demand circuit designation from the interface, use the **no** form of this command.

demand-circuit [**disable** | **enable**]

no demand-circuit

Syntax Description

disable	(Optional) Disables the interface as an OSPF demand circuit.
enable	(Optional) Enables the interface as an OSPF demand circuit.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the demand circuit parameter specified by the area.
 If this command is not specified in area configuration mode, then the interface adopts the demand circuit parameter specified for the process.
 If this command is not specified at any level, then the circuit is not a demand circuit.

Command Modes

Interface configuration
 Area configuration
 Router configuration
 VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	The disable keyword was added.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

On point-to-point interfaces, only one end of the demand circuit must be configured with this command. Periodic hello messages are suppressed and periodic refreshes of link-state advertisements (LSAs) do not flood the demand circuit. Use the **demand-circuit** command to allow the underlying data link layer to be closed when the topology is stable. In point-to-multipoint topology, only the multipoint end must be configured with this command.

Task ID

Task ID	Operations
ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to set the configuration for an OSPF demand circuit:

```
RP/0/RP0/CPU0:router# configure  
RP/0/RP0/CPU0:router(config)# router ospf 1  
RP/0/RP0/CPU0:router(config-ospf)# demand-circuit
```

R3.3 Beta Draft – Cisco Confidential Information

disable-dn-bit-check

To specify that down bits should be ignored, use the **disable-dn-bit-check** command in VPN Routing and Forwarding (VRF) configuration mode. To specify that down bits should be considered, use the **no** form of this command.

- **disable-dn-bit-check**
- **no disable-dn-bit-check**

Syntax Description	This command has no arguments or keywords.

Defaults	Down bits are considered.

Command Modes	VRF configuration mode

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	ospf	read, write

Examples	The following example shows how to specify that down bits be ignored: <pre>RP/0/RP0/CPU0:router# configure RP/0/RP0/CPU0:router(config)# router ospf 1 RP/0/RP0/CPU0:router(config-ospf)# vrf v1 RP/0/RP0/CPU0:router(config-ospf-vrf)# disable-dn-bit-check</pre>

R3.3 Beta Draft—Cisco Confidential Information

distance (IP)

To define an administrative distance, use the **distance** command in router configuration mode. To remove the **distance** command from the configuration file and restore the system to its default condition in which the software removes a distance definition, use the **no** form of this command.

distance *weight* [*ip-address mask* [*access-list-name*]]

no distance *weight ip-address mask* [*access-list-name*]

Syntax Description

<i>weight</i>	Administrative distance. Range is 1 to 255. Used alone, the <i>weight</i> argument specifies a default administrative distance that the software uses when no other specification exists for a routing information source. Routes with a distance of 255 are not installed in the routing table. Table 68 lists the default administrative distances.
<i>ip-address</i>	(Optional) IP address in four-part, dotted-decimal notation.
<i>mask</i>	(Optional) IP address mask in four-part, dotted-decimal format. A bit set to 1 in the <i>mask</i> argument instructs the software to ignore the corresponding bit in the address value.
<i>access-list-name</i>	(Optional) Name of an IP access list to be applied to incoming routing updates.

Defaults

If this command is not specified at the area level, then the administrative distance is the default, as specified in [Table 68](#).

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The <i>ip-address</i> and <i>mask</i> arguments for the no form of the command were changed from optional to required.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information

An administrative distance is an integer from 10 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means that the routing information source cannot be trusted at all and should be ignored. Weight values are subjective; no quantitative method exists for choosing weight values.

If an access list is used with this command, it is applied when a network is being inserted into the routing table. This behavior allows you to filter networks based on the IP address of the router supplying the routing information. For example, you could filter possibly incorrect routing information from networking devices not under your administrative control.

The order in which you enter **distance** commands can affect the assigned administrative distances in unexpected ways (see the “Examples” section for further clarification).

Table 68 lists default administrative distances.

Table 68 Default Administrative Distances

Route Source	Default Distance
Connected interface	0
Static route	1
External Border Gateway Protocol (BGP)	20
OSPF	110
IS-IS	115
Internal BGP	200
Unknown	255

Task ID

Task ID	Operations
ospf	read, write

Examples

In the following example, the **router ospf** command sets up OSPF routing in autonomous system number 1. The first **distance** command sets the default administrative distance to 255, which instructs the software to ignore all routing updates from networking devices for which an explicit distance has not been set. The second **distance** command sets the administrative distance for all networking devices on the Class C network 192.168.40.0 to 90.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# distance 255
RP/0/RP0/CPU0:router(config-ospf)# distance 90 192.168.40.0 0.0.0.255
```

Related Commands

Command	Description
distance bgp	Allows the use of external, internal, and local administrative distances that could be a better route to a BGP node.
distance ospf	Allows the use of external, internal, and local administrative distances that could be a better route to an OSPF node.
router ospf	Configures the OSPF routing process.

R3.3 Beta Draft—Cisco Confidential Information

distance ospf

To define Open Shortest Path First (OSPF) route administrative distances based on route type, use the **distance ospf** command in router configuration mode. To restore the default value, use the **no** form of this command.

distance ospf {intra-area | inter-area | external} *distance*

no distance ospf

Syntax Description	intra-area inter-area external	Sets the type of area. It can be one of the following values: intra-area—All routes within an area. inter-area—All routes from one area to another area. external—All routes from other routing domains, learned by redistribution.
	<i>distance</i>	Route administrative distance.

Defaults *distance*: 110

Command Modes Router configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You must specify one of the keywords.

Use the **distance ospf** command to perform the same function as the **distance** command used with an access list. However, the **distance ospf** command sets a distance for an entire group of routes, rather than a specific route that passes an access list.

A common reason to use the **distance ospf** command is when you have multiple OSPF processes with mutual redistribution, and you want to prefer internal routes from one over external routes from the other.

Task ID	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples The following example shows how to change the external distance to 200, making the route less reliable:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# redistribute ospf 2
RP/0/RP0/CPU0:router(config-ospf)# distance ospf external 200
RP/0/RP0/CPU0:router(config-ospf)# exit
RP/0/RP0/CPU0:router(config)# router ospf 2
RP/0/RP0/CPU0:router(config-ospf)# redistribute ospf 1
RP/0/RP0/CPU0:router(config-ospf)# distance ospf external 200
```

Related Commands	Command	Description
	disable-dn-bit-check	Defines an administrative distance.

R3.3 Beta Draft—Cisco Confidential Information

distribute-list

To filter networks received or transmitted in Open Shortest Path First (OSPF) updates, use the **distribute-list** command in the appropriate mode. To change or cancel the filter, use the **no** form of this command.

distribute-list *access-list-name* {**in** | **out** [**bgp** | **connected** | **ospf** | **static**]}

no distribute-list *access-list-name* {**in** | **out**}

Syntax Description

<i>access-list-name</i>	Standard IP access list name. The list defines which networks are to be received and which are to be suppressed in routing updates.
in	Applies the access list to incoming routing updates.
out	Applies the access list to outgoing routing updates. The out keyword is available only in router configuration mode.
bgp	(Optional) Applies the access list to BGP routes.
connected	(Optional) Applies the access list to connected routes.
ospf	(Optional) Applies the access list to OSPF routes (not the current OSPF process).
static	(Optional) Applies the access list to statically configured routes.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the distribute list parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the distribute list parameter specified for the process.

If this command is not specified at any level, then the distribute list is disabled.

Command Modes

Interface configuration
Area configuration
Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft–Cisco Confidential Information

Use the **distribute-list** command to limit which OSPF routes are installed on this router. The **distribute-list** command does not affect the OSPF protocol itself.

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows how to prevent OSPF routes from the 172.17.10.0 network from being installed if they are learned in area 0:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv4 access-list 3
RP/0/RP0/CPU0:router(config-ipv4-acl)# deny 172.17.10.0 0.0.0.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit any any
!
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# distribute-list 3 in
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/1/0/3
```


R3.3 Beta Draft—Cisco Confidential Information

domain-id

To specify the Open Shortest Path First (OSPF) VPN Routing and Forwarding (VRF) domain ID, use the **domain-id** command in VRF configuration mode. To remove an OSPF VRF domain ID, use the **no** form of this command.

domain-id [**secondary**] **type** [0005 | 0105 | 0205 | 8005] **value** *value*

no domain-id [**secondary**] **type** [0005 | 0105 | 0205 | 8005] **value** *value*

Syntax Description

secondary	(Optional) OSPF secondary domain-id.
type	Primary OSPF domain ID in hex format.
value <i>value</i>	OSPF domain ID value in hex format (six octets).

Defaults

No domain ID is specified.

Command Modes

VRF configuration mode

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The OSPF domain ID helps OSPF determine how to translate a prefix received through Border Gateway Protocol (BGP) from the remote Provider Edge (PE). If the domain IDs match, OSPF generates a Type 3 link state advertisement (LSA). If the domain IDs do not match, OSPF generates a Type 5 LSA.

There is only one primary domain ID. There can be multiple secondary domain IDs.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to specify a domain ID:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 01
RP/0/RP0/CPU0:router(config-ospf)# vrf v1
RP/0/RP0/CPU0:router(config-ospf-vrf)# domain-id type 0105 value AABBCDDDEEFF
```

R3.3 Beta Draft – Cisco Confidential Information

domain-tag

To specify the Open Shortest Path First (OSPF) VPN Routing and Forwarding (VRF) domain tag, use the **domain-tag** command in VRF configuration mode. To remove an OSPF VRF domain tag, use the **no** form of this command.

domain-tag *tag*

no domain-tag

Syntax Description	<i>tag</i>	OSPF domain tag as a 32-bit value. The valid range is 0 to 4294967295.

Defaults	No OSPF VRF domain tag is specified.	

Command Modes	VRF configuration mode	

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .	
	The domain tag is added to any Type 5 link state advertisements (LSAs) generated as a result of VPN-IP routes received from Border Gateway Protocol (BGP).	

Task ID	Task ID	Operations
	ospf	read, write

Examples	The following example shows how to specify the domain tag:	
	RP/0/RP0/CPU0:router# configure	
	RP/0/RP0/CPU0:router(config)# router ospf 01	
	RP/0/RP0/CPU0:router(config-ospf)# domain-tag 234	

R3.3 Beta Draft—Cisco Confidential Information

flood-reduction (OSPF)

To suppress the unnecessary flooding of link-state advertisements (LSAs) in stable topologies, use the **flood-reduction** command in the appropriate mode. To remove this functionality from the configuration, use the **no** form of this command.

flood-reduction [**enable** | **disable**]

no flood-reduction [**enable** | **disable**]

Syntax Description

enable	(Optional) Turns on this functionality at a specific level.
disable	(Optional) Turns off this functionality at a specific level.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the flood reduction parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the flood reduction parameter specified for the process.

If this command is not specified at any level, then flood reduction is disabled.

Command Modes

Interface configuration
Area configuration
Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

All routers supporting the OSPF demand circuit are compatible and can interact with routers supporting flooding reduction.

Task ID

Task ID	Operations
ospf	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to reduce the flooding of unnecessary LSAs for area 0:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/1/0/3
RP/0/RP0/CPU0:router(config-ospf-ar-if)# flood-reduction
```

Related Commands

Command	Description
show ospf interface	Displays OSPF-related interface information.
show ospf neighbor	Displays OSPF neighbor information on an individual interface basis.

R3.3 Beta Draft—Cisco Confidential Information

hello-interval (OSPF)

To specify the interval between hello packets that are sent on the Open Shortest Path First (OSPF) interface, use the **hello-interval** command in the appropriate mode. To return to the default time, use the **no** form of this command.

hello-interval *seconds*

no hello-interval

Syntax Description

<i>seconds</i>	Interval (in seconds). The value must be the same for all nodes on a specific network. Range is 1 to 65535.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the hello interval parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the hello interval parameter specified for the process.

If this command is not specified at any level, then the hello interval is 10 seconds (broadcast) or 30 seconds (nonbroadcast).

Command Modes

Interface configuration
Area configuration
Router configuration
Virtual-link configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The hello interval value is advertised in the hello packets. The shorter the hello interval, the faster topological changes are detected, but more routing traffic occurs. This value must be the same for all routers and access servers on a specific network.

Task ID

Task ID	Operations
ospf	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to set the interval between hello packets to 15 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-ospf-ar-if)# hello-interval 15
```

Related Commands

Command	Description
dead-interval (OSPF)	Sets the time period for which hello packets are suspended before neighbors declare the router down.

R3.3 Beta Draft—Cisco Confidential Information

ignore lsa mospf

To suppress the sending of syslog messages when the router receives link-state advertisement (LSA) Type 6 multicast Open Shortest Path First (MOSPF) packets, which are unsupported, use the **ignore lsa mospf** command in router configuration mode. To restore the sending of syslog messages, use the **no** form of this command.

ignore lsa mospf

no ignore lsa mospf

Syntax Description

This command has no arguments or keywords.

Defaults

When you do not specify this command in router configuration mode, each MOSPF packet received by the router causes the router to send a syslog message.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Cisco routers do not support LSA Type 6 (MOSPF), and they generate syslog messages if they receive such packets. If the router is receiving many MOSPF packets, you might want to configure the router to ignore the packets and thus prevent a large number of syslog messages.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure the router to suppress the sending of syslog messages when it receives MOSPF packets:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# ignore lsa mospf
```

R3.3 Beta Draft—Cisco Confidential Information

interface (OSPF)

To define the interfaces on which the Open Shortest Path First (OSPF) protocol runs, use the **interface** command in area configuration mode. To disable OSPF routing for interfaces, use the **no** form of this command.

interface *type instance*

no interface *type instance*

Syntax Description

<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults

When you do not specify this command in configuration mode, OSPF routing for interfaces is not enabled.

Command Modes

Area configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information

Use the **interface** command to associate a specific interface with an area. The interface remains associated with the area even when the IP address of the interface changes.

Task ID	Task ID	Operations
	ospf	read, write

Examples The following example shows how the OSPF routing process 109 defines four OSPF areas (0, 2, 3, and 10.9.50.0), and associates an interface with each area:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 109
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS4/0/0/3
!
RP/0/RP0/CPU0:router(config-ospf)# area 2
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/1/0/3
!
RP/0/RP0/CPU0:router(config-ospf)# area 3
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS3/0/0/2
!
RP/0/RP0/CPU0:router(config-ospf)# area 10.9.50.0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS3/0/0/1
```

R3.3 Beta Draft – Cisco Confidential Information

log adjacency changes (OSPF)

To configure the router to send a syslog message when the state of an Open Shortest Path First (OSPF) neighbor changes, use the **log adjacency changes** command in router configuration mode. To turn off this function, use the **disable** keyword. To log all state changes, use the **detail** keyword.

log adjacency changes [**detail** | **disable**]

Syntax Description	detail	(Optional) Provides detailed information about adjacency changes.
	disable	(Optional) Disables sending adjacency change messages.

Defaults	The router sends a syslog message when the state of an OSPF neighbor changes.

Command Modes	Router configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the log adjacency changes command to display high-level changes to the state of the peer relationship. Configure this command if you want to know about OSPF neighbor changes.

Task ID	Task ID	Operations
	ospf	read, write

Examples	The following example shows how to configure the software to send a syslog message for any OSPF neighbor state changes:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 109
RP/0/RP0/CPU0:router(config-ospf)# log adjacency changes enable
```

R3.3 Beta Draft—Cisco Confidential Information

max-metric

To configure the Open Shortest Path First (OSPF) protocol to signal other networking devices not to prefer the local router as an intermediate hop in their shortest path first (SPF) calculations, use the **max-metric** command in router configuration mode. To disable this function, use the **no** form of this command.

max-metric router-lsa [**on-startup** { **wait-for-bgp** | *announce-time* }]

no max-metric router-lsa

Syntax Description		
router-lsa		Always originates router link-state advertisements (LSAs) with the maximum metric.
on-startup		(Optional) Sets the maximum metric temporarily after a reboot.
wait-for-bgp		(Optional) Causes OSPF to originate router LSAs with the maximum metric and allows Border Gateway Protocol (BGP) to decide when to start originating router LSAs with a normal metric instead of the maximum metric.
<i>announce-time</i>		(Optional) The time (in seconds) that router LSAs are originated with the maximum metric of 0XFFFF.

Defaults	Router LSAs are originated with normal link metrics.

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

Use the **max-metric** command to cause the software to originate router LSAs with router link metrics set to LSInfinity (0XFFFF). This feature can be useful in Internet backbone routers that run both OSPF and BGP because OSPF converges more quickly than BGP and may begin attracting traffic before BGP has converged, resulting in dropped traffic.

If this command is configured, the router advertises its locally generated router LSAs with a metric of 0XFFFF. This action allows the router to converge but not attract transit traffic if there are better, alternative paths around this router. After the specified *announce-time* value or notification from BGP has expired, the router advertises the local router LSAs with the normal metric (interface cost).

R3.3 Beta Draft – Cisco Confidential Information

If this command is configured with the **on-startup** keyword, then the maximum metric is temporarily set only after reboot is initiated. If this command is configured without the **on-startup** keyword, then the maximum metric is permanently used until the configuration is removed.

This command might be useful when you want to connect a router to an OSPF network, but do not want real traffic flowing through it if there are better, alternative paths. If there are no alternative paths, this router still accepts transit traffic as before.

Some cases where this command might be useful are as follows:

- During a router reload, you prefer that OSPF wait for BGP to converge before accepting transit traffic. If there are no alternative paths, the router still accepts transit traffic.
- A router is in critical condition (for example, it has a very high CPU load or does not have enough memory to store all LSAs or build the routing table).
- When you want to gracefully introduce or remove a router to or from the network.
- When you have a test router in a lab, connected to a production network.



Note

For older OSPF implementations (RFC 1247), router links in received router LSAs with a metric and cost of LSInfinity are not used during SPF calculations. Hence, no transit traffic is set to the routers originating such router LSAs.

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows how to configure OSPF to originate router LSAs with the maximum metric until BGP indicates that it has converged:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 109
RP/0/RP0/CPU0:router(config-ospf)# max-metric router-lsa on-startup wait-for-bgp
```

R3.3 Beta Draft—Cisco Confidential Information

maximum interfaces (OSPF)

To limit the number of interfaces that can be configured for an Open Shortest Path First (OSPF) process, use the **maximum interfaces** command in router configuration mode. To return to the default limit, use the **no** form of this command.

maximum interfaces *number-interfaces*

no maximum interfaces

Syntax Description

number-interfaces Number of interfaces. Range is 1 to 1024.

Defaults

If the command is not specified, the default is 255.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **maximum interface** command to increase or decrease the limit on the number of interfaces configured for an OSPF process.

You cannot configure a limit lower than the number of interfaces currently configured for the OSPF process. To lower the limit, remove interfaces from the OSPF configuration until the number of configured interfaces is at or below the desired limit. You may then apply the new, lower limit.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure a maximum interface limit of 700 on a router:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 109
RP/0/RP0/CPU0:router(config-ospf)# maximum interfaces 700
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	show ospf interface	Displays OSPF interface information.

R3.3 Beta Draft—Cisco Confidential Information

maximum paths (OSPF)

To control the maximum number of parallel routes that the Open Shortest Path First (OSPF) protocol can support, use the **maximum paths** command in router configuration mode. To remove the **maximum paths** command from the configuration file and restore the system to its default condition with respect to the routing protocol, use the **no** form of this command.

maximum paths *maximum*

no maximum paths

Syntax Description	<i>maximum</i>	Maximum number of parallel routes that OSPF can install in a routing table. Range is 1 to 32 for Cisco CRS-1s and 1 to 16 for Cisco XR 12000 Series Routers.

Defaults	Cisco CRS-1s: 32 paths Cisco XR 12000 Series Routers: 16 paths

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	ospf	read, write

Examples	The following example shows how to allow a maximum of two paths to a destination:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 109
RP/0/RP0/CPU0:router(config-ospf)# maximum paths 2
```

R3.3 Beta Draft—Cisco Confidential Information

maximum redistributed-prefixes (OSPF)

To limit the aggregate number of routes that may be redistributed into an Open Shortest Path First (OSPF) process, use the **maximum redistributed-prefix** command in router configuration mode. To return to the default limit, use the **no** form of this command.

maximum redistributed-prefixes *maximum* [*threshold-value*] [**warning-only**]

no maximum redistributed-prefixes

Syntax Description

<i>maximum</i>	Number of routes. Range is 1 to 28672.
<i>threshold-value</i>	(Optional) Threshold value (as a percentage) at which to generate a warning message. Range is 1 to 100.
warning-only	(Optional) Gives only a warning when the limit is exceeded.

Defaults

If the command is not specified, the default is 10000.
The threshold value defaults to 75%.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	The <i>threshold-value</i> argument and warning-only keyword were added.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **maximum redistributed-prefixes** command to increase or decrease the maximum number of routes redistributed for an OSPF process.

If the *maximum* value is less than the existing number of routes, existing routes remain configured, but no new routes are redistributed.

Task ID

Task ID	Operations
ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure a maximum number of routes that can be redistributed for an OSPF routing process:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 109
RP/0/RP0/CPU0:router(config-ospf)# maximum redistributed-prefixes 15000
```

Related Commands

Command	Description
show ospf route	Displays the OSPF topology table.

R3.3 Beta Draft—Cisco Confidential Information

message-digest-key

To enable Open Shortest Path First (OSPF) Message Digest 5 (MD5) authentication, use the **message-digest-key** command in the appropriate mode. To remove an old MD5 key, use the **no** form of this command.

message-digest-key *key-id* **md5** {*key* | **clear** *key* | **encrypted** *key*}

no message-digest-key *key-id*

Syntax Description

<i>key-id</i>	Key number. Range is 1 to 255.
md5	Enables OSPF MD5 authentication.
<i>key</i>	Alphanumeric string of up to 16 characters.
clear	Specifies that the key be clear text.
encrypted	Specifies that the key be encrypted using a two-way algorithm.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the message digest key parameter specified by the area.
 If this command is not specified in area configuration mode, then the interface adopts the message digest key parameter specified for the process.
 If this command is not specified at any level, then OSPF MD5 authentication is disabled.

Command Modes

Interface configuration
 Area configuration
 Router configuration
 Virtual-link configuration
 VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The 0 and 7 keywords were replaced with the clear and encrypted keywords.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Usually, one key individual interface is used to generate authentication information when packets are sent and to authenticate incoming packets. The same key identifier on the neighbor router must have the same *key* value.

R3.3 Beta Draft—Cisco Confidential Information

For authentication to be enabled, you must configure the **message-digest-key** command together with the **authentication** command and its **message-digest** keyword. Both the **message-digest-key** and **authentication** commands can be inherited from a higher configuration level.

The process of changing keys is as follows. Suppose the current configuration is:

```
interface POS 0/3/0/2
 message-digest-key 100 md5 OLD
```

You change the configuration to the following:

```
interface POS 0/3/0/2
 message-digest-key 101 md5 NEW
```

The system assumes its neighbors do not have the new key yet, so it begins a rollover process. It sends multiple copies of the same packet, each authenticated by different keys. In this example, the system sends out two copies of the same packet—the first one authenticated by key 100 and the second one authenticated by key 101.

Rollover allows neighboring routers to continue communication while the network administrator is updating them with the new key. Rollover stops after the local system finds that all its neighbors know the new key. The system detects that a neighbor has the new key when it receives packets from the neighbor authenticated by the new key.

After all neighbors have been updated with the new key, the old key should be removed. In this example, you would enter the following:

```
interface ethernet 1
 no ospf message-digest-key 100
```

Then, only key 101 is used for authentication on interface 1.

We recommend that you not keep more than one key individual interface. Every time you add a new key, you should remove the old key to prevent the local system from continuing to communicate with a hostile system that knows the old key. Removing the old key also reduces overhead during rollover.



Note

The MD5 key is always stored in encrypted format on the router. The **clear** and **encrypted** keywords inform the router whether the value that is entered is encrypted or unencrypted.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to set a new key 19 with the password 8ry4222:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 109
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-ospf-ar-if)# message-digest-key 19 md5 8ry4222
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	authentication (OSPF)	Enables plain text, MD5 authentication, or null authentication for an OSPF interface.
	area (OSPF)	Configures an OSPF area.
	default-cost (OSPF)	Enables authentication for an OSPF area.

R3.3 Beta Draft—Cisco Confidential Information

mpls ldp sync (OSPF)

To enable Label Distribution Protocol (LDP)-Interior Gateway Protocol (IGP) synchronization, use the **mpls ldp sync** command in Router configuration mode. To disable LDP-IGP synchronization, use the **no** form of this command.

mpls ldp sync

no ospf ldp sync

Syntax Description	This command has no arguments or keywords.

Defaults	LDP-IGP synchronization is disabled for OSPF.

Command Modes	Router configuration mode

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	ospf	read, write

Examples	The following example shows how to enable LDP-IGP synchronization:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 01
RP/0/RP0/CPU0:router(config-ospf)# mpls ldp sync
```

R3.3 Beta Draft – Cisco Confidential Information

mpls traffic-eng area (OSPF)

To configure an Open Shortest Path First (OSPF) area for Multiprotocol Label Switching traffic engineering (MPLS TE), use the **mpls traffic-eng area** command in router configuration mode. To remove the MPLS TE area, use the **no** form of this command.

```
mpls traffic-eng area area-id

no mpls traffic-eng area area-id
```

Syntax Description	area-id	Integer that specifies an OSPF area in which MPLS TE is supported. Currently only one area is supported.

Defaults	MPLS TE is not configured for OSPF.

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You must configure the **mpls traffic-eng area** command for OSPF to support MPLS traffic engineering. OSPF provides the flooding mechanism that is used to flood TE link information.

We recommend that you configure the **mpls traffic-eng router-id** command instead of using the **router-id** command in global configuration mode.

OSPF support for MPLS TE is a component of the overall MPLS TE feature. Other MPLS TE software components must also be configured for this feature to be fully supported.

Task ID	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to associate loopback interface 0 with area 0, and area 0 is declared to be an MPLS area:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# router-id 10.10.10.10
RP/0/RP0/CPU0:router(config-ospf)# mpls traffic-eng router-id loopback 0
RP/0/RP0/CPU0:router(config-ospf)# mpls traffic-eng area 0
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface loopback 0
```

Related Commands

Command	Description
capability opaque	Controls the OSPF opaque LSA support capability.
mpls traffic-eng router-id (OSPF)	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.
router-id (OSPF)	Configures a router ID for the OSPF process.

R3.3 Beta Draft—Cisco Confidential Information

mpls traffic-eng router-id (OSPF)

To specify that the traffic engineering router identifier for the node is the IP address associated with a given Open Shortest Path First (OSPF) interface, use the **mpls traffic-eng router-id** command in router configuration mode. To disable this feature, use the **no** form of this command.

mpls traffic-eng router-id { *router-id* | *interface-type interface-instance* }

no mpls traffic-eng router-id { *ip-address* | *interface-type interface-number* }

Syntax Description

<i>router-id</i>	The 32-bit router ID value specified in four-part, dotted-decimal notation (must be in the valid IP address range of 0.0.0.0 to 255.255.255.255).
<i>interface-type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults

If this command is specified in router configuration mode, then the traffic engineering router identifier for the node is the IP address associated with a given interface.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

This identifier of the router acts as a stable IP address for the traffic engineering configuration. This IP address is flooded to all nodes. For all traffic engineering tunnels originating at other nodes and ending at this node, you must set the tunnel destination to the traffic engineering router identifier of the destination node, because that is the address that the traffic engineering topology database at the tunnel head uses for its path calculation.



Note

We recommend that loopback interfaces be used for Multiprotocol Label Switching traffic engineering (MPLS TE) because they are more stable than physical interfaces.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to specify the traffic engineering router identifier as the IP address associated with loopback interface 0:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# mpls traffic-eng router-id loopback 0
```

Related Commands

Command	Description
mpls traffic-eng area (OSPF)	Configures an OSPF area for MPLS TE.

R3.3 Beta Draft—Cisco Confidential Information

mtu-ignore (OSPF)

To prevent Open Shortest Path First (OSPF) from checking whether neighbors are using the same maximum transmission unit (MTU) on a common interface when exchanging database descriptor (DBD) packets, use the **mtu-ignore** command in the appropriate mode. To reset to default, use the **no** form of this command.

```
mtu-ignore [disable | enable]

no mtu-ignore
```

Syntax Description	disable	(Optional) Enables checking for whether OSPF neighbors are using the MTU on a common interface.
	enable	(Optional) Disables checking for whether OSPF neighbors are using the MTU on a common interface.

Defaults	If this command is not specified in interface configuration mode, then the interface adopts the MTU ignore parameter specified by the area. If this command is not specified in area configuration mode, then the interface adopts the MTU ignore parameter specified for the process. If this command is not specified at any level, then OSPF checks the MTU received from neighbors when exchanging DBD packets.

Command Modes	Interface configuration Area configuration Router configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	The disable keyword was added.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the mtu-ignore command with the enable keyword to check whether OSPF neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DBD packets. If the receiving MTU in the DBD packet is higher than the MTU configured on the incoming interface, OSPF adjacency is not established.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	ospf	read, write

Examples The following example shows how to disable MTU mismatch detection on receiving DBD packets:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 109
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/1/0/3
RP/0/RP0/CPU0:router(config-ospf-ar-if)# mtu-ignore
```

R3.3 Beta Draft—Cisco Confidential Information

neighbor (OSPF)

To configure Open Shortest Path First (OSPF) routers interconnecting to nonbroadcast networks, use the **neighbor** command in interface configuration mode. To remove a configuration, use the **no** form of this command.

neighbor *ip-address* [**cost** *number*] [**priority** *number*] [**poll-interval** *seconds*]

no neighbor *ip-address* [**cost** *number*] [**priority** *number*] [**poll-interval** *seconds*]

Syntax Description	
<i>ip-address</i>	Interface IP address of the neighbor.
cost <i>number</i>	(Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured assume the cost of the interface, based on the cost command. On point-to-multipoint interfaces, cost <i>number</i> is the only keyword and argument combination that works. The cost keyword does not apply to nonbroadcast multiaccess (NBMA) networks.
priority <i>number</i>	(Optional) Specifies an 8-bit number indicating the router priority value of the nonbroadcast neighbor associated with the IP address specified. The priority keyword does not apply to point-to-multipoint interfaces.
poll-interval <i>seconds</i>	(Optional) Specifies an unsigned integer value (in seconds) reflecting the poll interval. RFC 1247 recommends that this value be much larger than the hello interval. The poll-interval keyword does not apply to point-to-multipoint interfaces.

Defaults	No configuration is specified. priority <i>number</i>: 0 poll-interval <i>seconds</i>: 120 seconds (2 minutes)

Command Modes	Interface configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. You must include one neighbor entry in the software configuration for each known nonbroadcast network neighbor. The neighbor address must be on the primary address of the interface.

R3.3 Beta Draft—Cisco Confidential Information

If a neighboring router has become inactive (hello packets have not been received for the router dead interval period), it may still be necessary to send hello packets to the dead neighbor. These hello packets are sent at a reduced rate called the *poll interval*.

When the router starts up, it sends only hello packets to those routers with nonzero priority; that is, routers that are eligible to become designated routers (DRs) and backup designated routers (BDRs). After the DR and BDR are selected, the DR and BDR start sending hello packets to all neighbors to form adjacencies.

To filter all outgoing OSPF link-state advertisement (LSA) packets for the neighbor, use the **neighbor database-filter all out** command.

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows how to declare a router at address 172.16.3.4 on a nonbroadcast network, with a priority of 1 and a poll interval of 180 seconds:

```
RP/0/0/0:router(config-ospf-ar-if)# neighbor 172.16.3.4 priority 1 poll-interval 180
```

The following example illustrates a network with nonbroadcast:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS1/0/0/3
RP/0/RP0/CPU0:router(config-if)# ip address 172.16.3.10 255.255.255.0

RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS1/0/0/3
RP/0/RP0/CPU0:router(config-ospf-ar-if)# network nonbroadcast
RP/0/RP0/CPU0:router(config-ospf-ar-if)# neighbor 172.16.3.4 priority 1 poll-interval 180
RP/0/RP0/CPU0:router(config-ospf-ar-if)# neighbor 172.16.3.5 cost 10 priority 1
poll-interval 180
RP/0/RP0/CPU0:router(config-ospf-ar-if)# neighbor 172.16.3.6 cost 15 priority 1
poll-interval 180
RP/0/RP0/CPU0:router(config-ospf-ar-if)# neighbor 172.16.3.7 priority 1 poll-interval 180
```

Related Commands	Command	Description
	neighbor database-filter all out	Filters all outgoing LSAs to an OSPF neighbor.
	network (OSPF)	Configures the OSPF network type to a type other than the default for a given medium.
	priority (OSPF)	Sets the router priority, which helps determine the designated router for this network.

R3.3 Beta Draft—Cisco Confidential Information

neighbor database-filter all out

To filter all outgoing link-state advertisements (LSAs) to an Open Shortest Path First (OSPF) neighbor, use the **neighbor database-filter all out** command in interface configuration mode. To restore the forwarding of LSAs to the neighbor, use the **no** form of this command.

neighbor ip-address database-filter all out

no neighbor ip-address database-filter all out

Syntax Description	ip-address	IP address of the neighbor to which outgoing LSAs are blocked.

Defaults	Instead of all outgoing LSAs being filtered to the neighbor, they are flooded to the neighbor.

Command Modes	Interface configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the neighbor database-filter all out command to filter all outgoing OSPF LSA packets during synchronization and flooding for point-to-multipoint neighbors on nonbroadcast networks. More neighbor options are available with the neighbor command.

Task ID	Task ID	Operations
	ospf	read, write

Examples	The following example shows how to prevent flooding of OSPF LSAs from point-to-multipoint networks to the neighbor at IP address 10.2.3.4:
	RP/0/RP0/CPU0:router# configure
	RP/0/RP0/CPU0:router(config)# router ospf 1
	RP/0/RP0/CPU0:router(config-ospf)# area 0
	RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS1/0/0/3
	RP/0/RP0/CPU0:router(config-ospf-ar-if)# neighbor 10.2.3.4 database-filter all out

R3.3 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
neighbor (OSPF)	Configures OSPF routers interconnecting to nonbroadcast networks.

R3.3 Beta Draft—Cisco Confidential Information

network (OSPF)

To configure the Open Shortest Path First (OSPF) network type to a type other than the default for a given medium, use the **network** command in the appropriate mode. To return to the default value, use the **no** form of this command.

network { **broadcast** | **non-broadcast** | { **point-to-multipoint** [**non-broadcast**] | **point-to-point** } }

no network

Syntax Description

broadcast	Sets the network type to broadcast.
non-broadcast	Sets the network type to nonbroadcast multiaccess (NBMA).
point-to-multipoint	Sets the network type to point-to-multipoint.
non-broadcast	(Optional) Sets the point-to-multipoint network to be nonbroadcast. If you use this keyword, the neighbor command is required.
point-to-point	Sets the network type to point-to-point.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the network parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the network parameter specified for the process.

If this command is not specified at any level, then the OSPF network type is the default of the given medium.

POS interfaces default to point-to-point and GigE and TenGigE interfaces default to broadcast.

Command Modes

Interface configuration
Area configuration
Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **network** command to configure broadcast networks as NBMA networks when, for example, routers in your network do not support multicast addressing.

R3.3 Beta Draft—Cisco Confidential Information

Configuring NBMA networks as either broadcast or nonbroadcast assumes that there are virtual circuits from every router to every router or fully meshed network. However, there are other configurations where this assumption is not true; for example, a partially meshed network. In these cases, you can configure the OSPF network type as a point-to-multipoint network. Routing between two routers that are not directly connected go through the router that has virtual circuits to both routers. You need not configure neighbors when using this command.

If this command is issued on an interface that does not allow it, this command is ignored.

OSPF has two features related to point-to-multipoint networks. One feature applies to broadcast networks; the other feature applies to nonbroadcast networks:

- On point-to-multipoint, broadcast networks, you can use the **neighbor** command, and you must specify a cost to that neighbor.
- On point-to-multipoint, nonbroadcast networks, you must use the **neighbor** command to identify neighbors. Assigning a cost to a neighbor is optional.

Task ID	Task ID	Operations
	ospf	read, write

Examples	The following example shows how to configure the OSPF network as a nonbroadcast network: <pre> RP/0/RP0/CPU0:router# configure RP/0/RP0/CPU0:router(config)# router ospf 1 RP/0/RP0/CPU0:router(config-ospf)# area 0 RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/1/0/3 RP/0/RP0/CPU0:router(config-ospf-ar-if)# network non-broadcast RP/0/RP0/CPU0:router(config-ospf-ar-if)# neighbor 172.16.3.4 priority 1 poll-interval 180 </pre>

Related Commands	Command	Description
	neighbor (OSPF)	Configures OSPF routers interconnecting to nonbroadcast networks.

R3.3 Beta Draft—Cisco Confidential Information

nsf (OSPF)

To configure nonstop forwarding (NSF) for the Open Shortest Path First (OSPF) protocol, use the **nsf** command in router configuration mode. To remove this command from the configuration file and restore the system to its default condition, use the **no** form of this command.

```
nsf { cisco [enforce global] | ietf [helper disable] }

no nsf { [cisco [enforce global] | ietf [helper disable] }
```

Syntax Description

cisco	Enables Cisco Nonstop Forwarding.
enforce global	(Optional) Cancels NSF restart when non-NSF network device neighbors are detected.
ietf	Enables Internet Engineering Task Force (IETF) graceful restart.
helper disable	(Optional) Disables router helper support.

Defaults

NSF is disabled.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The NSF feature allows for the forwarding of data packets to continue along known routes while routing protocol information (such as OSPF) is being restored following a switchover.

Use the **nsf** command if the router is expected to perform NSF during restart. To experience the full benefits of this feature, configure all neighboring routers with NSF.

When this command is used without the optional **cisco enforce global** keywords and non-NSF neighbors are detected, the NSF restart mechanism aborts on the interfaces of those neighbors and functions properly on others.

When this command is used with the optional **cisco enforce global** keywords and non-NSF neighbors are detected, NSF restart is canceled for the entire OSPF process.

R3.3 Beta Draft—Cisco Confidential Information

IETF restart provides an NSF mechanism to allow data traffic to flow seamlessly with no packet drops during the transient period when OSPF attempts to recover after a process restart or RP failover, within the guidelines of RFC 3623.

By default, neighbors in helper mode listen to both the NSF Cisco- and NSF IETF-type LSAs. The **nsf** command enables one type of mechanism that would undergo an RP failover or, anticipating an OSPF process restart. If the **cisco** or **ietf** keyword is not entered, NSF is not enabled, irrespective of neighbors in listening mode for both NSF Cisco and NSF IETF.

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows how to cancel NSF restart for the entire OSPF process if non-NSF neighbors are detected on any network interface during restart:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# nsf cisco enforce global
```

R3.3 Beta Draft – Cisco Confidential Information

nsf interval (OSPF)

To configure the minimum time between nonstop forwarding (NSF) restart attempts for the Open Shortest Path First (OSPF) protocol, use the **nsf interval** command in router configuration mode. To remove this command from the configuration file and restore the system to its default condition, use the **no** form of this command.

```

nsf interval seconds

no nsf interval seconds
    
```

Syntax Description	<i>seconds</i>	Length of time (in seconds) between restart attempts. Range is 90 to 3600 seconds.

Defaults	<i>seconds</i> : 90

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. When you use the nsf interval command, the OSPF process must be up for at least 90 seconds before OSPF attempts to perform an NSF restart.

Task ID	Task ID	Operations
	ospf	read, write

Examples	The following example shows how to configure the minimum time between NSF restart attempts at 120 seconds: <pre> RP/0/RP0/CPU0:router# configure RP/0/RP0/CPU0:router(config)# router ospf 1 RP/0/RP0/CPU0:router(config-ospf)# nsf interval 120 </pre>

R3.3 Beta Draft—Cisco Confidential Information

nsf lifetime (OSPF)

To configure the maximum time that routes are held in the Routing Information Base (RIB) following an Open Shortest Path First (OSPF) process restart, use the **nsf lifetime** command in router configuration mode. To remove this command from the configuration file and restore the system to its default condition, use the **no** form of this command.

nsf lifetime *seconds*

no nsf lifetime *seconds*

Syntax Description	<i>seconds</i>	The length of time (in seconds) that routes are held in the RIB. Range is 90 to 3600 seconds.

Defaults	<i>seconds</i> : 90

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

When you use this command, the OSPF process must reconverge within the maximum length of time configured. If the convergence exceeds this length of time, routes are purged from RIB and nonstop forwarding (NSF) restart may fail.

Task ID	Task ID	Operations
	ospf	read, write

Examples	The following example shows how to configure the maximum lifetime for OSPF NSF at 120 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# nsf lifetime 120
```

R3.3 Beta Draft—Cisco Confidential Information

nssa (OSPF)

To configure an area as a not-so-stubby area (NSSA), use the **nssa** command in area configuration mode. To remove the NSSA distinction from the area, use the **no** form of this command.

nssa [**no-redistribution**] [**default-information-originate**] [**no-summary**]

no nssa

Syntax Description

no-redistribution	(Optional) Imports routes only into the normal areas, but not into the NSSA area, by the redistribute command when the router is an NSSA Area Border Router (ABR).
default-information-originate	(Optional) Generates a Type 7 default into the NSSA area. This keyword takes effect only on an NSSA ABR or NSSA Autonomous System Boundary Router (ASBR).
no-summary	(Optional) Prevents an ABR from sending summary link advertisements into the NSSA.

Defaults

No NSSA area is defined.

Command Modes

Area configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

An NSSA does not flood Type 5 external LSAs from the core into the area, but can import autonomous system external routes in a limited fashion within the area.

Task ID

Task ID	Operations
ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure area 1 as an NSSA area:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# area 1
RP/0/RP0/CPU0:router(config-ospf-ar)# nssa
```

R3.3 Beta Draft – Cisco Confidential Information

ospf name-lookup

To configure the Open Shortest Path First (OSPF) protocol to look up Domain Name System (DNS) names, use the **ospf name-lookup** command in global configuration mode. To disable this function, use the **no** form of this command.

```
ospf name-lookup

no ospf name-lookup
```

Syntax Description This command has no arguments or keywords.

Defaults Routers are displayed by router ID or neighbor ID.

Command Modes Global configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **ospf name-lookup** command to easily identify a router when executing all OSPF **show** command displays. The router is displayed by name rather than by its router ID or neighbor ID.

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows how to configure OSPF to identify a router by name:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ospf name-lookup
```


R3.3 Beta Draft—Cisco Confidential Information

packet-size

To configure the size of Open Shortest Path First (OSPF) packets up to the size specified by the maximum transmission unit (MTU), use the **packet-size** command in the appropriate router configuration mode. To disable this function and reestablish the default packet size, use the **no** form of this command.

packet-size *bytes*

no packet-size

Syntax Description	<i>bytes</i>	Size in bytes. Range is 576 to 10000 bytes.

Defaults	If command is not specified, the default packet size is 1500 bytes.

Command Modes	Router configuration Area configuration Interface configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **packet-size** command to customize the size of OSPF packets. The OSPF protocol compares the packet size and the MTU size and uses the lower packet size value.

Task ID	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure the packet size on an interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS1/0/0/2
RP/0/RP0/CPU0:router(config-ospf-ar-if)# packet-size 3500
```

R3.3 Beta Draft—Cisco Confidential Information

passive (OSPF)

To suppress the sending of Open Shortest Path First (OSPF) protocol operation on an interface, use the **passive** command in the appropriate configuration mode. To remove the passive configuration, use the **no** form of this command.

passive [**enable** | **disable**]

no passive

Syntax Description

enable	(Optional) Suppresses OSPF updates.
disable	(Optional) Sends OSPF updates.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the passive parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the passive parameter specified for the process.

If this command is not specified at any level, then the passive parameter is disabled and OSPF updates are sent on the interface.

Command Modes

Interface configuration
Area configuration
Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

OSPF routing information is neither sent nor received through the specified interface. The interface appears as a stub network in the OSPF Router (Type 1) link-state advertisement (LSA).

Task ID

Task ID	Operations
ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows that Packet-over-SONET/SDH (POS) interface 1/0/0/2 reduces OSPF updates because passive mode is enabled; however, POS interface 0/1/0/3 receives normal OSPF traffic flow:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS1/0/0/2
RP/0/RP0/CPU0:router(config-ospf-ar-if)# passive enable
RP/0/RP0/CPU0:router(config-ospf-ar-if)# exit
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS1/0/0/3
RP/0/RP0/CPU0:router(config-ospf-ar-if)# end
```

R3.3 Beta Draft—Cisco Confidential Information

priority (OSPF)

To set the router priority for an interface, which helps determine the designated router for an Open Shortest Path First (OSPF) link, use the **priority** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

priority *value*

no priority *value*

Syntax Description

<i>value</i>	8-bit unsigned integer indicating the router priority value. Range is 0 to 255.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the priority parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the priority parameter specified for the process.

If this command is not specified at any level, then the default priority is 1.

Command Modes

Interface configuration
Area configuration
Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multiaccess networks (in other words, not point-to-point networks).

This priority value is used when you configure the Open Shortest Path First (OSPF) protocol for nonbroadcast networks using the **neighbor** command for OSPF.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	ospf	read, write

Examples The following example shows that priority is set through the **priority** and **neighbor** commands for Routers A and B and that the neighbor priority value must reflect that of the neighbor router:

Router A

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.0.0.2 255.255.255.0
RP/0/RP0/CPU0:router(config-if)# exit
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-ospf-ar-if)# network non-broadcast
RP/0/RP0/CPU0:router(config-ospf-ar-if)# priority 4
RP/0/RP0/CPU0:router(config-ospf-ar-if)# neighbor 10.0.0.1 priority 6
```

Router B

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/1
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.0.0.1 255.255.255.0
RP/0/RP0/CPU0:router(config-if)# exit
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/2/0/1
RP/0/RP0/CPU0:router(config-ospf-ar-if)# network non-broadcast
RP/0/RP0/CPU0:router(config-ospf-ar-if)# priority 6
RP/0/RP0/CPU0:router(config-ospf-ar-if)# neighbor 10.0.0.2 priority 4
```

Related Commands	Command	Description
	neighbor (OSPF)	Configures OSPF routers interconnecting to nonbroadcast networks.
	network (OSPF)	Configures the OSPF network type to a type other than the default for a given medium.

R3.3 Beta Draft—Cisco Confidential Information

range (OSPF)

To consolidate and summarize routes at an area boundary, use the **range** command in area configuration mode. To disable this function, use the **no** form of this command.

range *ip-address mask* [**advertise** | **not-advertise**]

no range *address mask* [**advertise** | **not-advertise**]

Syntax Description

<i>ip-address</i>	IP address in four-part, dotted-decimal notation.
<i>mask</i>	IP address mask.
advertise	(Optional) Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA).
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed and the component networks remain hidden from other networks.

Defaults

When this command is not specified for Area Border Routers (ABRs), routes at an area boundary are not consolidated or summarized.
Advertise is the default.

Command Modes

Area configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **range** command only with Area Border Router (ABRs). Use the command to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This process is called *route summarization*.

Multiple range configurations specifying the **range** command can be configured. Thus, the OSPF protocol can summarize addresses for many different sets of address ranges.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows area 36.0.0.0 consisting of interfaces whose IP addresses have “10.31.x.x” as the first two octets. The **range** command summarizes interfaces. Instead of advertising eight networks individually, the single route 10.31.0.0 255.255.0.0 is advertised:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 201
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar-if)# interface POS 0/3/0/2
!
RP/0/RP0/CPU0:router(config-ospf)# area 36.0.0.0
RP/0/RP0/CPU0:router(config-ospf-ar)# range 10.31.0.0 255.255.0.0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS0/1/0/0
RP/0/RP0/CPU0:router(config-ospf-ar-if)# interface POS0/1/0/0
RP/0/RP0/CPU0:router(config-ospf-ar-if)# interface POS0/1/0/1
RP/0/RP0/CPU0:router(config-ospf-ar-if)# interface POS0/1/0/2
RP/0/RP0/CPU0:router(config-ospf-ar-if)# interface POS0/1/0/3
RP/0/RP0/CPU0:router(config-ospf-ar-if)# interface POS0/2/0/0
RP/0/RP0/CPU0:router(config-ospf-ar-if)# interface POS0/2/0/1
RP/0/RP0/CPU0:router(config-ospf-ar-if)# interface POS0/2/0/2
RP/0/RP0/CPU0:router(config-ospf-ar-if)# interface POS0/2/0/3
RP/0/RP0/CPU0:router(config-ospf-ar-if)# end
```


R3.3 Beta Draft—Cisco Confidential Information**redistribute (OSPF)**

To redistribute routes from one routing domain into Open Shortest Path First (OSPF), 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 in which the software does not redistribute routes, use the **no** form of this command.

Border Gateway Protocol (BGP)

redistribute bgp *process-id* [**metric** *metric-value*] [**metric-type** {1 | 2}] [**route-policy** *policy-name*] [**tag** *tag-value*]

no redistribute bgp *process-id* [**metric** *metric-value*] [**metric-type** {1 | 2}] [**route-policy** *policy-name*] [**tag** *tag-value*]

Local Interface Routes

redistribute connected [**metric** *metric-value*] [**metric-type** {1 | 2}] [**route-policy** *policy-name*] [**tag** *tag-value*]

no redistribute connected [**metric** *metric-value*] [**metric-type** {1 | 2}] [**route-policy** *policy-name*] [**tag** *tag-value*]

Enhanced Interior Gateway Routing Protocol (EIGRP)

redistribute eigrp *process-id* [**match** {external [1 | 2] | internal | nssa-external [1 | 2]] [**metric** *metric-value*] [**metric-type** {1 | 2}] [**route-policy** *policy-name*] [**tag** *tag-value*]

no redistribute eigrp *process-id* [**match** {external [1 | 2] | internal | nssa-external [1 | 2]] [**metric** *metric-value*] [**metric-type** {1 | 2}] [**route-policy** *policy-name*] [**tag** *tag-value*]

Intermediate System-to-Intermediate System (IS-IS)

redistribute isis *process-id* [**level-1** | **level-2** | **level-1-2**] [**metric** *metric-value*] [**metric-type** {1 | 2}] [**route-policy** *policy-name*] [**tag** *tag-value*]

no redistribute isis *process-id* [**level-1** | **level-2** | **level-1-2**] [**metric** *metric-value*] [**metric-type** {1 | 2}] [**route-policy** *policy-name*] [**tag** *tag-value*]

Open Shortest Path First (OSPF)

redistribute ospf *process-id* [**match** {external [1 | 2] | internal | nssa-external [1 | 2]] [**metric** *metric-value*] [**metric-type** {1 | 2}] [**route-policy** *policy-name*] [**tag** *tag-value*]

no redistribute ospf *process-id* [**match** {external [1 | 2] | internal | nssa-external [1 | 2]] [**metric** *metric-value*] [**metric-type** {1 | 2}] [**route-policy** *policy-name*] [**tag** *tag-value*]

Routing Information Protocol (RIP)

redistribute rip [**metric** *metric-value*] [**metric-type** {1 | 2}] [**route-policy** *policy-name*] [**tag** *tag-value*]

no redistribute rip [**metric** *metric-value*] [**metric-type** {1 | 2}] [**route-policy** *policy-name*] [**tag** *tag-value*]

R3.3 Beta Draft—Cisco Confidential Information

IP Static Routes

redistribute static [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]

no redistribute static [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]

Syntax Description		
bgp		Distributes routes from the BGP protocol.
<i>process-id</i>		For the bgp keyword, an autonomous system number, which is a 16-bit decimal number. Range is 1 to 65535. For the isis keyword, an IS-IS instance name from which routes are to be redistributed. The value takes the form of a string. A decimal number can be entered, but it is stored internally as a string. For the ospf keyword, an OSPF instance name from which routes are to be redistributed. The value takes the form of a string. A decimal number can be entered, but it is stored internally as a string.
metric <i>metric-value</i>		(Optional) Specifies the metric used for the redistributed route. Range is 1 to 16777214. Use a value consistent with the source protocol.
metric-type { 1 2 }		(Optional) Specifies the external link type associated with the route advertised into the OSPF routing domain. It can be one of two values: • 1—Type 1 external route • 2—Type 2 external route
tag <i>tag-value</i>		(Optional) Specifies the 32-bit dotted-decimal value attached to each external route. This value is not used by the OSPF protocol itself, but is carried in the External LSAs. Range is 0 to 4294967295.
route-policy <i>policy-name</i>		(Optional) Specifies the identifier of a configured policy. A policy is used to filter the importation of routes from this source routing protocol to OSPF.
connected		Distributes routes that are established automatically by virtue of having enabled IP on an interface.
eigrp		Distribute routes from the EIGRP protocol.
isis		Distributes routes from the IS-IS protocol.
level-1		(Optional) Redistributes Level 1 routes into other IP routing protocols independently.
level-1-2		(Optional) Distributes both Level 1 and Level 2 routes into other IP routing protocols.
level-2		(Optional) Distributes Level 2 routes into other IP routing protocols independently.
ospf		Distributes routes from the OSPF protocol.

R3.3 Beta Draft—Cisco Confidential Information

match {internal external [1 2] nssa-external [1 2]}	(Optional) Specifies the criteria by which OSPF routes are redistributed into other routing domains. It can be one or more of the following: • internal—Routes that are internal to a specific autonomous system (intra- and inter-area OSPF routes). • external [1 2]—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 external routes. • nssa-external [1 2]—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 not-so-stubby area (NSSA) external routes. For the external and nssa-external options, if a type is not specified, then both Type 1 and Type 2 are assumed. If no match is specified, the default is no filtering.
rip	Distributes routes from the RIP protocol.
static	Distributes IP static routes.

Defaults

Route redistribution is disabled.

metric *metric-value*: Default is 20 for routes from all protocols except BGP routes, for which the default is 1.

metric-type: Type 2 external route

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode. The policy keyword was changed to route-policy. The eigrp and rip keywords were added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Redistributed routing information should always be filtered by the **policy** *policy-name* keyword and argument. This filtering ensures that only those routes intended by the administrator are redistributed by OSPF.

For information about routing policies, see the *Routing Policy Commands on Cisco IOS XR Software* module of the *Cisco IOS XR Routing Command Reference*.

R3.3 Beta Draft—Cisco Confidential Information

OSPF Considerations

Whenever you use the **redistribute** or **default-information originate (OSPF)** command 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 between OSPF processes, no OSPF metrics are preserved.

When routes are redistributed into OSPF and no metric is specified with the **metric** keyword, OSPF uses 20 as the default metric for routes from all protocols except BGP routes, which get a metric of 1.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to cause BGP routes to be redistributed into an OSPF domain:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 110
RP/0/RP0/CPU0:router(config-ospf)# redistribute bgp 100
```

The following example shows how to redistribute the specified IS-IS process routes into an OSPF domain. The IS-IS routes are redistributed with a metric of 100.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 109
RP/0/RP0/CPU0:router(config-ospf)# redistribute isis 108 metric 100
```

In the following example, network 10.0.0.0 appears as an external link-state advertisement (LSA) in OSPF 1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-if)# ip address 10.0.0.0 255.0.0.0
!
RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/2
RP/0/RP0/CPU0:router(config)# ip address 10.99.0.0 255.0.0.0
!
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# redistribute ospf 2
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/2/0/2
!
RP/0/RP0/CPU0:router(config)# router ospf 2
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/1/0/1
```

Related Commands

Command	Description
default-information originate (OSPF)	Generates a default external route into an OSPF routing domain.

R3.3 Beta Draft—Cisco Confidential Information

retransmit-interval (OSPF)

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the Open Shortest Path First (OSPF) interface, use the **retransmit-interval** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

retransmit-interval *seconds*

no retransmit-interval

Syntax Description

<i>seconds</i>	Time (in seconds) between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network. Range is 1 to 65535 seconds.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the retransmit interval parameter specified by the area.
 If this command is not specified in area configuration mode, then the interface adopts the retransmit interval parameter specified for the process.
 If this command is not specified at any level, then the default retransmit interval is 5 seconds.

Command Modes

Interface configuration
 Area configuration
 Router configuration
 Virtual-link configuration
 VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When a router sends an LSA to its neighbor, it keeps the LSA until it receives the acknowledgment message. If the router receives no acknowledgment, it resends the LSA.

The setting of this parameter should be conservative, or needless retransmission results. The value should be larger for serial lines and virtual links.

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	ospf	read, write

Examples The following example shows how to set the retransmit interval value to 8 seconds in interface configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 201
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/2/0/1
RP/0/RP0/CPU0:router(config-ospf-ar-if)# retransmit-interval 8
```

R3.3 Beta Draft—Cisco Confidential Information**router-id (OSPF)**

To configure a router ID for the Open Shortest Path First (OSPF) process, use the **router-id** command in router configuration mode. To cause the software to use the default method of determining the router ID, use the **no** form of this command.

router-id {*router-id* | *interface-type interface-instance*}

no router-id {*router-id* | *interface-type interface-instance*}

Syntax Description		
	<i>router-id</i>	32-bit router ID value specified in four-part, dotted-decimal notation.
	<i>interface-type</i>	Interface type. For more information, use the question mark (?) online help function.
	<i>interface-instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults	If this command is not configured, the router ID is the highest IP version 4 (IPv4) address for an interface on the router, with any loopback interface taking precedence.

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was added under the VRF configuration mode.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

It is good practice to use the **router-id** command to explicitly specify a unique 32-bit numeric value for the router ID. This action ensures that OSPF can function regardless of the interface address configuration.

OSPF attempts to obtain a router ID from the following sources, in order of decreasing preference:

1. The 32-bit numeric value specified by the OSPF **router-id** command in router configuration mode. (This value can be any 32-bit value. It is not restricted to the IPv4 addresses assigned to interfaces on this router, and need not be a routable IPv4 address.)
2. The primary IPv4 address of the interface specified by the OSPF **router-id** command.
3. The 32-bit numeric value specified by the **router-id** command in global configuration mode. (This value must be an IPv4 address assigned to an interface on this router.)
4. The primary IPv4 address of the interface specified by the **router-id** command in global configuration mode.
5. The highest IPv4 address assigned to any loopback interface.
6. The primary IPv4 address of an interface over which this OSPF process is running.



Note

Unlike OSPF version 3, OSPF version 2 is guaranteed to have at least one interface with an IPv4 address configured.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to assign the IP address of 172.20.10.10 to the OSPF process 109:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 109
RP/0/RP0/CPU0:router(config-ospf)# router-id 172.20.10.10
```

Related Commands

Command	Description
clear ospf process	Resets an OSPF router process without stopping and restarting it.
ipv4 address	Sets a primary IPv4 address for an interface.

R3.3 Beta Draft—Cisco Confidential Information

router ospf

To configure an Open Shortest Path First (OSPF) routing process, use the **router ospf** command in global configuration mode. To terminate an OSPF routing process, use the **no** form of this command.

router ospf *process-name*

no router ospf *process-name*

Syntax Description

<i>process-name</i>	Name that uniquely identifies an OSPF routing process. The process name is any alphanumeric string no longer than 40 characters without spaces.

Defaults

No OSPF routing process is defined.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You can specify multiple OSPF routing processes in each router.

All OSPF configuration commands must be configured under an OSPF routing process. For example, two of these commands are the **default-metric** command and the **router-id** command.

Task ID

Task ID	Operations
ospf	read, write
rib	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to instantiate an OSPF routing process called 109:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 109
```

Related Commands

Command	Description
area (OSPF)	Defines an OSPF area.
default-metric (OSPF)	Sets default metric values for routes redistributed from another protocol into the OSPF protocol.
interface (OSPF)	Defines the interfaces on which the OSPF protocol runs.
router-id (OSPF)	Configures a router ID for the OSPF process.

R3.3 Beta Draft—Cisco Confidential Information

show ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the **show ospf** command in EXEC mode.

show ospf [*process-name*] [**vrf** [*vrf-name* | **all**]]

Syntax Description

<i>process-name</i>	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the router ospf command. If this argument is included, only information for the specified routing process is displayed.
vrf <i>vrf-name</i>	(Optional) Identifier of an OSPF VPN Routing and Forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as an arbitrary string. The strings 'default' and 'all' are reserved <i>vrf-names</i> .
all	(Optional) Displays information for all VRFs defined on an OSPF routing process.

Defaults

IPv4 and unicast address prefixes

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show ospf** command to provide basic information about the OSPF processes running on the router. Additional options provide in-depth information.

Task ID

Task ID	Operations
ospf	Read

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following is sample output from the **show ospf** command:

```
RP/0/RP0/CPU0:router# show ospf

Routing Process "ospf 1" with ID 1.1.1.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
It is an area border router
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPF's 10000 msecs
Maximum wait time between two consecutive SPF's 10000 msecs
Initial LSA throttle delay 500 msecs
Minimum hold time for LSA throttle 5000 msecs
Maximum wait time for LSA throttle 5000 msecs
Minimum LSA interval 5000 msecs. Minimum LSA arrival 1 secs
Maximum number of configured interfaces 255
Number of external LSA 0. Checksum Sum 00000000
Number of opaque AS LSA 0. Checksum Sum 00000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 2. 2 normal 0 stub 0 nssa
External flood list length 0
Non-Stop Forwarding enabled
  Area BACKBONE(0) (Inactive)
    Number of interfaces in this area is 2
    SPF algorithm executed 8 times
    Number of LSA 2. Checksum Sum 0x01ba83
    Number of opaque link LSA 0. Checksum Sum 00000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
  Area 1
    Number of interfaces in this area is 1
    SPF algorithm executed 9 times
    Number of LSA 2. Checksum Sum 0x0153ea
    Number of opaque link LSA 0. Checksum Sum 00000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

Table 69 describes the significant fields shown in the display.

Table 69 show ospf Field Descriptions

Field	Description
Routing Process “ospf 201” with ID 172.22.110.200	OSPF process name.
Supports only	Number of types of service supported (Type 0 only).
It is	Types are internal, area border, or autonomous system boundary.
Redistributing External Routes from	Lists of redistributed routes, by protocol.
SPF schedule delay	Delay time of SPF calculations.
Minimum LSA interval	Minimum interval between LSAs.
Minimum LSA arrival	Minimum elapsed time between accepting an update for the same link-state advertisement (LSA).

R3.3 Beta Draft—Cisco Confidential Information**Table 69** *show ospf Field Descriptions (continued)*

Field	Description
external LSA	Total number of Type 5 LSAs in the LSDB.
opaque LSA	Total number of Type 10 LSAs in the LSDB.
DCbitless...AS LSA	Total number of Demand Circuit Type 5 and Type 11 LSAs.
DoNotAge...AS LSA	Total number of Type 5 and Type 11 LSAs with the DoNotAge bit set.
Number of areas	Number of areas in router, area addresses, and so on.
Area BACKBONE	Backbone is area 0.

R3.3 Beta Draft – Cisco Confidential Information

show ospf border-routers

To display the internal Open Shortest Path First (OSPF) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the **show ospf border-routers** command in EXEC mode.

```
show ospf [process-name] [vrf vrf-name] border-routers [router-id]
```

Syntax Description	<i>process-name</i>	(Optional) OSPF process name. If this argument is included, only information for the specified routing process is included.
	vrf <i>vrf-name</i>	(Optional) Identifier of an OSPF VPN Routing and Forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as an arbitrary string. The strings ‘default’ and ‘all’ are reserved <i>vrf-names</i> .
	<i>router-id</i>	(Optional) Router ID associated with the border router. The <i>router-id</i> can be any 32-bit router ID value specified in four-part, dotted-decimal notation. No default exists.

Defaults IPv4 and unicast address prefixes

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The <i>router-id</i> argument was added.
	Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show ospf border-routers** command to list all OSPF border routers visible to the specified processes and also to ascertain the OSPF topology of the router.

Task ID	Task ID	Operations
	ospf	Read

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following is sample output from the **show ospf border-routers** command:

```
RP/0/RP0/CPU0:router# show ospf border-routers

OSPF 1 Internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 172.31.97.53 [1] via 172.16.1.53, POS 3/0/0/0, ABR/ASBR , Area 0, SPF 3
```

Table 70 describes the significant fields shown in the display.

Table 70 *show ospf border-routers Field Descriptions*

Field	Description
i	Type of this route; i indicates an intra-area route, I an interarea route.
172.31.97.53	Router ID of destination.
[1]	Cost of using this route.
172.16.1.53	Next hop toward the destination.
POS 3/0/0/0	Packets destined for 172.16.1.53 are sent over Packet-over-SONET/SDH (POS) interface 3/0/0/0.
ABR/ASBR	Router type of the destination; it is either an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR) or both.
Area 0	Area ID of the area from which this route is learned.
SPF 3	Internal number of the shortest path first (SPF) calculation that installs this route.

R3.3 Beta Draft—Cisco Confidential Information

show ospf database

To display lists of information related to the Open Shortest Path First (OSPF) database for a specific router, use the **show ospf database** command in EXEC mode.

```
show ospf [process-name] [vrf vrf-name] [area-id] database
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [adv-router ip-address]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [asbr-summary] [link-state-id]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [asbr-summary] [link-state-id]  
[adv-router ip-address]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [asbr-summary] [link-state-id]  
[self-originate]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [database-summary]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [external] [link-state-id]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [external] [link-state-id] [adv-router  
ip-address]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [external] [link-state-id]  
[self-originate]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [network] [link-state-id]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [network] [link-state-id] [adv-router  
ip-address]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [network] [link-state-id]  
[self-originate]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [nssa-external] [link-state-id]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [nssa-external] [link-state-id]  
[adv-router ip-address]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [nssa-external] [link-state-id]  
[self-originate]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [opaque-area] [link-state-id]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [opaque-area] [link-state-id]  
[adv-router ip-address]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [opaque-area] [link-state-id]  
[self-originate]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [opaque-as] [link-state-id]
```

```
show ospf [process-name] [vrf vrf-name] [area-id] database [opaque-as] [link-state-id]  
[adv-router ip-address]
```


R3.3 Beta Draft—Cisco Confidential Information

```

show ospf [process-name] [vrf vrf-name] [area-id] database [opaque-as] [link-state-id]
[self-originate]

show ospf [process-name] [vrf vrf-name] [area-id] database [opaque-link] [link-state-id]

show ospf [process-name] [vrf vrf-name] [area-id] database [opaque-link] [link-state-id]
[adv-router [ip-address]]

show ospf [process-name] [vrf vrf-name] [area-id] database [opaque-link] [link-state-id]
[self-originate]

show ospf [process-name] [vrf vrf-name] [area-id] database [router] [link-state-id]

show ospf [process-name] [vrf vrf-name] [area-id] database [router] [adv-router [ip-address]]

show ospf [process-name] [vrf vrf-name] [area-id] database [router] [self-originate]
[link-state-id]

show ospf [process-name] [vrf vrf-name] [area-id] database [self-originate]

show ospf [process-name] [vrf vrf-name] [area-id] database [summary] [link-state-id]

show ospf [process-name] [vrf vrf-name] [area-id] database [summary] [link-state-id]
[adv-router [ip-address]]

show ospf [process-name] [vrf vrf-name] [area-id] database [summary] [link-state-id]
[self-originate] [link-state-id]

```

Syntax Description	
<i>process-name</i>	(Optional) OSPF process name that uniquely identifies an OSPF routing process. The process name is any alphanumeric string no longer than 40 characters. If this argument is included, only information for the specified routing process is included.
vrf <i>vrf-name</i>	(Optional) Identifier of an OSPF VPN Routing and Forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as an arbitrary string. The strings 'default' and 'all' are reserved <i>vrf-names</i> .
<i>area-id</i>	(Optional) Area number used to define the particular area.
adv-router <i>ip-address</i>	(Optional) Displays all LSAs of the specified router.
asbr-summary	(Optional) Displays information only about the Autonomous System Boundary Router (ASBR) summary LSAs.

R3.3 Beta Draft—Cisco Confidential Information

<i>link-state-id</i>	(Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the link-state type of the advertisement. It must be entered in the form of an IP address. When the link-state advertisement (LSA) is describing a network, the <i>link-state-id</i> can take one of two forms: • The network IP address (as in Type 3 summary link advertisements and in autonomous system external link advertisements). • A derived address obtained from the link-state ID. Note Masking the link-state ID of a network link advertisement with the subnet mask of the network yields the IP address of the network. When the LSA is describing a router, the link-state ID is always the OSPF router ID of the described router. When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link-state ID is set to Default Destination (0.0.0.0).
self-originate	(Optional) Displays only self-originated LSAs (from the local router).
database-summary	(Optional) Displays how many of each type of LSA for each area there are in the database and the total.
external	(Optional) Displays information only about the external LSAs.
network	(Optional) Displays information only about the network LSAs.
nssa-external	(Optional) Displays information only about the not-so-stubby area (NSSA) external LSAs.
opaque-area	(Optional) Displays information about the opaque Type 10 LSAs. Type 10 denotes an area-local scope. Refer to RFC 2370 for more information on the opaque LSA options.
opaque-as	(Optional) Displays information about the opaque Type 11 LSAs. Type 11 denotes that the LSA is flooded throughout the autonomous system.
opaque-link	(Optional) Displays information about the opaque Type 9 LSAs. Type 9 denotes a link-local scope.
router	(Optional) Displays information only about the router LSAs.
summary	(Optional) Displays information only about the summary LSAs.

Defaults

IPv4 and unicast address prefixes

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The various forms of the **show ospf database** command deliver information about different OSPF link-state advertisements. This command can be used to examine the link-state database (LSD) and its contents. Each router participating in an area having identical database entries pertaining to that area (with the exception of LSAs that are being flooded). Numerous options (such as **network** and **router**) are used to display portions of the database.

Task ID

Task ID	Operations
ospf	Read

Examples

The following is sample output from the **show ospf database** command when no arguments or keywords are used:

```
RP/0/RP0/CPU0:router# show ospf database
```

```
OSPF Router with ID (172.20.1.11) (Process ID 1)
```

```
Router Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	Checksum	Link count
172.20.1.8	172.20.1.8	1381	0x8000010D	0xEF60	2
172.20.1.11	172.20.1.11	1460	0x800002FE	0xEB3D	4
172.20.1.12	172.20.1.12	2027	0x80000090	0x875D	3
172.20.1.27	172.20.1.27	1323	0x800001D6	0x12CC	3

```
Net Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	Checksum
172.22.1.27	172.20.1.27	1323	0x8000005B	0xA8EE
172.22.1.11	172.20.1.11	1461	0x8000005B	0x7AC

```
Type-10 Opaque Link Area Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	Checksum	Opaque ID
10.0.0.0	172.20.1.11	1461	0x800002C8	0x8483	0
10.0.0.0	172.20.1.12	2027	0x80000080	0xF858	0
10.0.0.0	172.20.1.27	1323	0x800001BC	0x919B	0
10.0.0.1	172.20.1.11	1461	0x8000005E	0x5B43	1

Table 71 describes the significant fields shown in the display.

Table 71 show ospf database Field Descriptions

Field	Description
Link ID	Router ID number.
ADV Router	ID of the advertising router.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Fletcher checksum of the complete contents of the LSA.

R3.3 Beta Draft—Cisco Confidential Information

Table 71 *show ospf database Field Descriptions (continued)*

Field	Description
Link count	Number of interfaces detected for the router.
Opaque ID	Opaque LSA ID number.

The following is sample output from the **show ospf database** command with the **asbr-summary** keyword:

```
RP/0/RP0/CPU0:router# show ospf database asbr-summary
```

```
OSPF Router with ID (192.168.0.1) (Process ID 300)
```

```
S    ummary ASB Link States (Area 0.0.0.0)
```

```

LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links (AS Boundary Router)
Link State ID: 172.17.245.1 (AS Boundary Router address)
Advertising Router: 172.17.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: /0
TOS: 0 Metric: 1
```

Table 72 describes the significant fields shown in the display.

Table 72 *show ospf database asbr-summary Field Descriptions*

Field	Description
OSPF Router with ID	Router ID number.
Process ID	OSPF process name.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID (ASBR).
Advertising Router	ID of the advertising router.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSAs.
Network Mask	Network mask implemented.
TOS	Type of service.
Metric	Link-state metric.

R3.3 Beta Draft—Cisco Confidential Information

The following is sample output from the **show ospf database** command with the **external** keyword:

```
RP/0/RP0/CPU0:router# show ospf database external

OSPF Router with ID (192.168.0.1) (Process ID 300)

      Type-5 AS External Link States

    LS age: 280
    Options: (No TOS-capability)
    LS Type: AS External Link
    Link State ID: 172.17.0.0 (External Network Number)
    Advertising Router: 172.17.70.6
    LS Seq Number: 80000AFD
    Checksum: 0xC3A
    Length: 36
    Network Mask: 255.255.0.0
      Metric Type: 2 (Larger than any link state path)
      TOS: 0
      Metric: 1
      Forward Address: 0.0.0.0
      External Route Tag: 0
```

Table 73 describes the significant fields shown in the display.

Table 73 *show ospf database external Field Descriptions*

Field	Description
OSPF Router with Router ID	Router ID number.
Process ID	OSPF process name.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID (external network number).
Advertising Router	ID of the advertising router.
LS Seq Number	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSA.
Network Mask	Network mask implemented.
Metric Type	External type.
TOS	Type of service.
Metric	Link-state metric.
Forward Address	Forwarding address. Data traffic for the advertised destination is forwarded to this address. If the forwarding address is set to 0.0.0.0, data traffic is forwarded instead to the originator of the advertisement.
External Route Tag	External route tag, a 32-bit field attached to each external route. This tag is not used by the OSPF protocol itself.

R3.3 Beta Draft—Cisco Confidential Information

The following is sample output from the **show ospf database** command with the **network** keyword:

```
RP/0/RP0/CPU0:router# show ospf database network

      OSPF Router with ID (192.168.0.1) (Process ID 300)

Net Link States (Area 0.0.0.0)

  LS age: 1367
  Options: (No TOS-capability)
  LS Type: Network Links
  Link State ID: 172.23.1.3 (address of Designated Router)
  Advertising Router: 192.168.0.1
  LS Seq Number: 800000E7
  Checksum: 0x1229
  Length: 52
  Network Mask: /24
    Attached Router: 192.168.0.1
    Attached Router: 172.23.241.5
    Attached Router: 172.23.1.1
    Attached Router: 172.23.54.5
    Attached Router: 172.23.1.5
```

Table 74 describes the significant fields shown in the display.

Table 74 *show ospf database network Field Descriptions*

Field	Description
OSPF Router with ID	Router ID number.
Process ID	OSPF process name.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID of the designated router.
Advertising Router	ID of the advertising router.
LS Seq Number	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSA.
Network Mask	Network mask implemented.
Attached Router	List of routers attached to the network, by IP address.

The following is sample output, carrying Multiprotocol Label Switching traffic engineering (MPLS TE) specification information, from the **show ospf database** command with the **opaque-area** keyword with a *link-state-id* of adv-router:

```
RP/0/RP0/CPU0:router# show ospf database opaque-area adv-router 172.20.1.12

      OSPF Router with ID (172.20.1.11) (Process ID 1)

Type-10 Opaque Link Area Link States (Area 0)

  LS age: 224
  Options: (No TOS-capability, DC)
```

R3.3 Beta Draft—Cisco Confidential Information

```

LS Type: Opaque Area Link
Link State ID: 10.0.0.0
Opaque Type: 1
Opaque ID: 0
Advertising Router: 172.20.1.12
LS Seq Number: 80000081
Checksum: 0xF659
Length: 132
Fragment number : 0

MPLS TE router ID : 172.20.1.12

Link connected to Point-to-Point network
  Link ID : 172.20.1.11
  Interface Address : 172.21.1.12
  Neighbor Address : 172.21.1.11
  Admin Metric : 10
  Maximum bandwidth : 193000
  Maximum reservable bandwidth : 125000
  Number of Priority : 8
  Priority 0 : 125000      Priority 1 : 125000
  Priority 2 : 125000      Priority 3 : 125000
  Priority 4 : 125000      Priority 5 : 125000
  Priority 6 : 125000      Priority 7 : 100000
  Affinity Bit : 0x0

Number of Links : 1

```

Table 75 describes the significant fields shown in the display.

Table 75 *show ospf database opaque-area Field Descriptions*

Field	Description
OSPF Router with ID	Router ID number.
Process ID	OSPF process name.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID.
Opaque Type	Opaque link-state type.
Opaque ID	Opaque ID number.
Advertising Router	ID of the advertising router.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSA.
Fragment number	Arbitrary value used to maintain multiple traffic engineering LSAs.
Link ID	Link ID number.
Interface Address	ID address of the interface.
Neighbor Address	IP address of the neighbor.
Admin Metric	Administrative metric value used by MPLS TE.

R3.3 Beta Draft—Cisco Confidential Information

Table 75 *show ospf database opaque-area Field Descriptions (continued)*

Field	Description
Maximum bandwidth	Specifies maximum bandwidth (in kbps).
Maximum reservable bandwidth	Specifies maximum reservable bandwidth (in kbps).
Number of Priority	Priority number.
Affinity Bit	Used by MPLS TE.

The following is sample output from the **show ospf database** command with the **router** keyword:

```
RP/0/RP0/CPU0:router# show ospf database router

      OSPF Router with ID (192.168.0.1) (Process ID 300)

      Router Link States (Area 0.0.0.0)

LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 172.23.21.6
Advertising Router: 172.23.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
Number of Links: 8

Link connected to: another Router (point-to-point)
(Link ID) Neighboring Router ID: 172.23.21.5
(Link Data) Router Interface address: 172.23.21.6
Number of TOS metrics: 0
  TOS 0 Metrics: 2
```

Table 76 describes the significant fields shown in the display.

Table 76 *show ospf database router Field Descriptions*

Field	Description
OSPF Router with ID	Router ID number.
Process ID	OSPF process name.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID.
Advertising Router	ID of the advertising router.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSA.
AS Boundary Router	Definition of router type.

R3.3 Beta Draft—Cisco Confidential Information

Table 76 *show ospf database router Field Descriptions (continued)*

Field	Description
Number of Links	Number of active links.
Link ID	Link type.
Link Data	Router interface address.
TOS	Type of service metric (Type 0 only).

The following is sample output from **show ospf database** command with the **summary** keyword:

```
RP/0/RP0/CPU0:router# show ospf database summary

      OSPF Router with ID (192.168.0.1) (Process ID 300)

Summary Net Link States (Area 0.0.0.0)

LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links (Network)
Link State ID: 172.23.240.0 (Summary Network Number)
Advertising Router: 172.23.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: /24
      TOS: 0   Metric: 1
```

Table 77 describes the significant fields shown in the display.

Table 77 *show ospf database summary Field Descriptions*

Field	Description
OSPF Router with ID	Router ID number.
Process ID	OSPF process name.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID (summary network number).
Advertising Router	ID of the advertising router.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSA.
Network Mask	Network mask implemented.
TOS	Type of service.
Metric	Link-state metric.

R3.3 Beta Draft—Cisco Confidential Information

The following is sample output from **show ospf database** command with the **database-summary** keyword:

```
RP/0/RP0/CPU0:router# show ospf database database-summary

OSPF Router with ID (172.19.65.21) (Process ID 1)

Area 0 database summary
  LSA Type      Count   Delete   Maxage
  Router        2       0        0
  Network       1       0        0
  Summary Net   2       0        0
  Summary ASBR  0       0        0
  Type-7 Ext    0       0        0
  Opaque Link   0       0        0
  Opaque Area   0       0        0
  Subtotal      5       0        0

Process 1 database summary
  LSA Type      Count   Delete   Maxage
  Router        2       0        0
  Network       1       0        0
  Summary Net   2       0        0
  Summary ASBR  0       0        0
  Type-7 Ext    0       0        0
  Opaque Link   0       0        0
  Opaque Area   0       0        0
  Type-5 Ext    2       0        0
  Opaque AS     0       0        0
  Total         7       0        0
```

Table 78 describes the significant fields shown in the display.

Table 78 *show ospf database database-summary* Field Descriptions

Field	Description
LSA Type	Link-state type.
Count	Number of advertisements in that area for each link-state type.
Delete	Number of LSAs that are marked “Deleted” in that area.
Maxage	Number of LSAs that are marked “Maxaged” in that area.

R3.3 Beta Draft – Cisco Confidential Information

show ospf flood-list

To display a list of Open Shortest Path First (OSPF) link-state advertisements (LSAs) waiting to be flooded over an interface, use the **show ospf flood-list** command in EXEC mode.

show ospf [*process-name*] [**vrf** *vrf-name*] [*area-id*] **flood-list** *interface-type* *interface-instance*

Syntax Description		
<i>process-name</i>	(Optional) OSPF process name that uniquely identifies an OSPF routing process. The process name is any alphanumeric string no longer than 40 characters. If this argument is included, only information for the specified routing process is included.	
vrf <i>vrf-name</i>	(Optional) Identifier of an OSPF VPN Routing and Forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as an arbitrary string. The strings 'default' and 'all' are reserved <i>vrf-names</i> .	
<i>area-id</i>	(Optional) Area number used to define the particular area.	
<i>interface-type</i>	Interface type. For more information, use the question mark (?) online help function.	
<i>interface-instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.	

Defaults All interfaces.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show ospf flood-list** command to display LSAs in flood queue and queue length.

Flood list information is transient and normally the flood lists are empty.

Task ID

Task ID	Operations
ospf	Read

Examples

The following is sample output from the **show ospf flood-list** command for interface POS 3/0/0/0:

```
RP/0/RP0/CPU0:router# show ospf flood-list POS 3/0/0/0
```

```
Interface POS3/0/0/0, Queue length 20
Link state retransmission due in 12 msec
Displaying 6 entries from flood list:

Type  LS ID           ADV RTR           Seq NO           Age           Checksum
  5    10.2.195.0        200.0.0.163      0x80000009      0            0xFB61
  5    10.1.192.0        200.0.0.163      0x80000009      0            0x2938
  5    10.2.194.0        200.0.0.163      0x80000009      0            0x757
  5    10.1.193.0        200.0.0.163      0x80000009      0            0x1E42
  5    10.2.193.0        200.0.0.163      0x80000009      0            0x124D
  5    10.1.194.0        200.0.0.163      0x80000009      0            0x134C
```

Table 79 describes the significant fields shown in the display.

Table 79 show ospf flood-list Field Descriptions

Field	Description
POS3/0/0/0	Interface for which information is displayed.
Queue length	Number of LSAs waiting to be flooded.
Link state retransmission due in	Length of time (in milliseconds) before next link-state transmission.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of the advertising router.
Seq NO	Sequence number of the LSA.
Age	Age of the LSA (in seconds).
Checksum	Checksum of the LSA.

R3.3 Beta Draft – Cisco Confidential Information

show ospf interface

To display Open Shortest Path First (OSPF) interface information, use the **show ospf interface** command in EXEC mode.

show ospf [*process-name*] [**vrf** *vrf-name*] [*area-id*] **interface** [*type instance*]

Syntax Description	
<i>process-name</i>	(Optional) OSPF process name that uniquely identifies an OSPF routing process. The process name is any alphanumeric string no longer than 40 characters. If this argument is included, only information for the specified routing process is included.
vrf <i>vrf-name</i>	(Optional) Identifier of an OSPF VPN Routing and Forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as an arbitrary string. The strings 'default' and 'all' are reserved <i>vrf-names</i> .
<i>area-id</i>	(Optional) Area number used to define the particular area.
<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>instance</i>	(Optional) Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults All interfaces

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Release	Modification
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
ospf	Read

Examples

The following is sample output from the **show ospf interface** command when Packet-over-SONET/SDH (POS) interface 3/0/0/0 is specified:

```
RP/0/RP0/CPU0:router# show ospf interface POS3/0/0/0
```

```
POS3/0/0/0 is up, line protocol is up
  Internet Address 172.16.254.202/24, Area 0
  Process ID 1, Router ID 192.77.99.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.254.10, Interface address 172.16.254.10
  Backup Designated router (ID) 172.16.254.28, Interface address 172.16.254.28
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 3, maximum is 3
  Last flood scan time is 1 msec, maximum is 1 msec
  Neighbor Count is 8, Adjacent neighbor count is 2
    Adjacent with neighbor 172.16.254.28 (Backup Designated Router)
    Adjacent with neighbor 172.16.254.10 (Designated Router)
  Suppress hello for 0 neighbor(s)
```

Table 80 describes the significant fields shown in the display.

Table 80 show ospf interface Field Descriptions

Field	Description
POS	Status of the physical link.
line protocol	Operational status of the protocol.
Internet Address	Interface IP address, subnet mask, and area address.
Process ID	OSPF process ID, router ID, network type, and link-state cost.
Transmit Delay	Transmit delay, interface state, and router priority.
Designated Router	Designated router ID and respective interface IP address.
Backup Designated router	Backup designated router ID and respective interface IP address.
Timer intervals configured	Configuration of timer intervals.

R3.3 Beta Draft—Cisco Confidential Information**Table 80** *show ospf interface Field Descriptions (continued)*

Field	Description
Hello	Number of seconds until next hello packet is sent over this interface.
Index 1/1	Area and autonomous system flood indexes.
Next 0x0(0)	Next area and autonomous system flood information, data pointer, and index.
Last flood scan length	Length of last flood scan.
Last flood scan time	Time (in milliseconds) of last flood scan.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.
Suppress hello	Count of neighbors suppressing hello messages.

R3.3 Beta Draft—Cisco Confidential Information

show ospf mpls traffic-eng

To display information about the links and fragments available on the local router for traffic engineering, use the **show ospf mpls traffic-eng** command in EXEC mode.

```
show ospf [process-name] [vrf vrf-name] [area-id] [interface-type interface-instance] mpls  
traffic-eng {link | fragment}
```

Syntax Description

<i>process-name</i>	(Optional) OSPF process name that uniquely identifies an OSPF routing process. The process name is any alphanumeric string no longer than 40 characters. If this argument is included, only information for the specified routing process is included.
vrf <i>vrf-name</i>	(Optional) Identifier of an OSPF VPN Routing and Forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as an arbitrary string. The strings 'default' and 'all' are reserved <i>vrf-names</i> .
<i>area-id</i>	(Optional) Area number used to define the particular area.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
link	Provides detailed information about the links over which traffic engineering is supported on the local router.
fragment	Provides detailed information about the traffic engineering fragments on the local router.

Defaults

All links or fragments

Command Modes

EXEC

R3.3 Beta Draft—Cisco Confidential Information

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
ospf	Read

Examples

The following is sample output from the **show ospf mpls traffic-eng** command when the **link** keyword is specified:

```
RP/0/RP0/CPU0:router# show ospf mpls traffic-eng link

      OSPF Router with ID (10.10.10.10) (Process ID 1)

Area 0 has 2 MPLS TE links. Area instance is 67441.

Links in hash bucket 3.
  Link is associated with fragment 1. Link instance is 67441
    Link connected to Point-to-Point network
    Link ID : 10.10.10.8
    Interface Address : 10.10.10.2
    Neighbor Address : 10.10.10.3
    Admin Metric : 0
    Maximum bandwidth : 19440000
    Maximum global pool reservable bandwidth : 25000000
    Maximum sub pool reservable bandwidth : 3125000
    Number of Priority : 8
    Global pool unreserved BW
    Priority 0 : 25000000 Priority 1 : 25000000
    Priority 2 : 25000000 Priority 3 : 25000000
    Priority 4 : 25000000 Priority 5 : 25000000
    Priority 6 : 25000000 Priority 7 : 25000000
    Sub pool unreserved BW
    Priority 0 : 3125000 Priority 1 : 3125000
    Priority 2 : 3125000 Priority 3 : 3125000
    Priority 4 : 3125000 Priority 5 : 3125000
    Priority 6 : 3125000 Priority 7 : 3125000
    Affinity Bit : 0

Links in hash bucket 8.
  Link is associated with fragment 0. Link instance is 67441
    Link connected to Point-to-Point network
    Link ID : 10.1.1.1
    Interface Address : 10.10.25.4
    Neighbor Address : 10.10.25.5
    Admin Metric : 0
```

R3.3 Beta Draft—Cisco Confidential Information

```

Maximum bandwidth : 19440000
Maximum global pool reservable bandwidth : 25000000
Maximum sub pool reservable bandwidth   : 3125000
Number of Priority : 8
Global pool unreserved BW
Priority 0 :   25000000 Priority 1 :   25000000
Priority 2 :   25000000 Priority 3 :   25000000
Priority 4 :   25000000 Priority 5 :   25000000
Priority 6 :   25000000 Priority 7 :   25000000
Sub pool unreserved BW
Priority 0 :    3125000 Priority 1 :    3125000
Priority 2 :    3125000 Priority 3 :    3125000
Priority 4 :    3125000 Priority 5 :    3125000
Priority 6 :    3125000 Priority 7 :    3125000
Affinity Bit : 0

```

Table 81 describes the significant fields shown in the display.

Table 81 *show ospf mpls traffic-eng link Field Descriptions*

Field	Description
Link ID	Link type.
Interface address	IP address of the interface.
Neighbor address	IP address of the neighbor.
Admin Metric	Administrative distance metric value used by Multiprotocol Label Switching traffic engineering (MPLS TE).
Maximum bandwidth	Bandwidth capacity of the link (in kbps).
Maximum global pool reservable bandwidth	Maximum amount of bandwidth that is available for reservation in the global pool.
Maximum sub pool reservable bandwidth	Maximum amount of bandwidth that is available for reservation in the subpool.
Number of Priority	Priority number.
Global pool unreserved BW	Amount of unreserved bandwidth that is available in the global pool.
Sub pool unreserved BW	Amount of unreserved bandwidth that is available in the subpool.
Affinity Bit	Used by MPLS TE. Attribute values required for links carrying this tunnel. A 32-bit dotted-decimal number. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.

The following is sample output from the **show ospf mpls traffic-eng** command when the **fragment** keyword is specified:

```

RP/0/RP0/CPU0:router# show ospf mpls traffic-eng fragment

      OSPF Router with ID (10.10.10.10) (Process ID 1)

Area 0 has 2 MPLS TE fragment. Area instance is 67441.
MPLS router address is 10.10.10.10
Next fragment ID is 2

Fragment 0 has 1 link. Fragment instance is 67441.

```

R3.3 Beta Draft—Cisco Confidential Information

```

Fragment has 1 link the same as last update.
Fragment advertise MPLS router address
  Link is associated with fragment 0. Link instance is 67441
    Link connected to Point-to-Point network
    Link ID : 10.1.1.1
    Interface Address : 10.10.25.4
    Neighbor Address : 10.10.25.5
    Admin Metric : 0
    Maximum bandwidth : 19440000
    Maximum global pool reservable bandwidth : 25000000
    Maximum sub pool reservable bandwidth : 3125000
    Number of Priority : 8
    Global pool unreserved BW
    Priority 0 : 25000000 Priority 1 : 25000000
    Priority 2 : 25000000 Priority 3 : 25000000
    Priority 4 : 25000000 Priority 5 : 25000000
    Priority 6 : 25000000 Priority 7 : 25000000
    Sub pool unreserved BW
    Priority 0 : 3125000 Priority 1 : 3125000
    Priority 2 : 3125000 Priority 3 : 3125000
    Priority 4 : 3125000 Priority 5 : 3125000
    Priority 6 : 3125000 Priority 7 : 3125000
    Affinity Bit : 0

```

```

Fragment 1 has 1 link. Fragment instance is 67441.
Fragment has 0 link the same as last update.
  Link is associated with fragment 1. Link instance is 67441
    Link connected to Point-to-Point network
    Link ID : 10.10.10.8
    Interface Address : 10.10.10.2
    Neighbor Address : 10.10.10.3
    Admin Metric : 0
    Maximum bandwidth : 19440000
    Maximum global pool reservable bandwidth : 25000000
    Maximum sub pool reservable bandwidth : 3125000
    Number of Priority : 8
    Global pool unreserved BW
    Priority 0 : 25000000 Priority 1 : 25000000
    Priority 2 : 25000000 Priority 3 : 25000000
    Priority 4 : 25000000 Priority 5 : 25000000
    Priority 6 : 25000000 Priority 7 : 25000000
    Sub pool unreserved BW
    Priority 0 : 3125000 Priority 1 : 3125000
    Priority 2 : 3125000 Priority 3 : 3125000
    Priority 4 : 3125000 Priority 5 : 3125000
    Priority 6 : 3125000 Priority 7 : 3125000
    Affinity Bit : 0

```

Table 82 describes the significant fields shown in the display.

Table 82 *show ospf mpls traffic-eng fragment Field Descriptions*

Field	Description
Area instance	Number of times traffic engineering information or any link changed.
Link instance	Number of times any link changed.
Link ID	Link type.
Interface address	IP address of the interface.

R3.3 Beta Draft – Cisco Confidential Information

Table 82 *show ospf mpls traffic-eng fragment Field Descriptions (continued)*

Field	Description
Neighbor address	IP address of the neighbor.
Admin Metric	Administrative distance metric value used by MPLS TE.
Maximum bandwidth	Bandwidth capacity of the link (in kbps).
Maximum global pool reservable bandwidth	Maximum amount of bandwidth that is available for reservation in the global pool.
Maximum sub pool reservable bandwidth	Maximum amount of bandwidth that is available for reservation in the subpool.
Number of Priority	Priority number.
Global pool unreserved BW	Amount of unreserved bandwidth that is available in the global pool.
Sub pool unreserved BW	Amount of unreserved bandwidth that is available in the subpool.
Affinity Bit	Used by MPLS TE. Attribute values required for links carrying this tunnel. A 32-bit dotted-decimal number. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.

R3.3 Beta Draft—Cisco Confidential Information

show ospf neighbor

To display Open Shortest Path First (OSPF) neighbor information on an individual interface basis, use the **show ospf neighbor** command in EXEC mode.

show ospf [*process-name*] [**vrf** *vrf-name*] [*area-id*] **neighbor** [*interface-type interface-instance*] [*neighbor-id*] [**detail**]

Syntax Description	
<i>process-name</i>	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the router ospf command. If this argument is included, only information for the specified routing process is displayed.
vrf <i>vrf-name</i>	(Optional) Identifier of an OSPF VPN Routing and Forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as an arbitrary string. The strings 'default' and 'all' are reserved <i>vrf-names</i> .
<i>area-id</i>	(Optional) Area ID. If you do not specify an area, all areas are displayed.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
<i>neighbor-id</i>	(Optional) Neighbor ID.
detail	(Optional) Displays all neighbors given in detail (lists all neighbors).

Defaults All neighbors

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Release	Modification
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
ospf	Read

Examples

The following is sample output from the **show ospf neighbor** command showing two lines of summary information for each neighbor:

```
RP/0/RP0/CPU0:router# show ospf neighbor
```

Neighbors for OSPF

```
Neighbor ID    Pri  State           Dead Time   Address        Interface
192.168.199.137 1    FULL/DR         0:00:31    172.31.80.37   POS 0/3/0/2
    Neighbor is up for 18:45:22
192.168.48.1    1    FULL/DROTHER    0:00:33    192.168.48.1   POS 0/3/0/3
    Neighbor is up for 18:45:30
192.168.48.200  1    FULL/DROTHER    0:00:33    192.168.48.200 POS 0/3/0/3
    Neighbor is up for 18:45:25
192.168.199.137 5    FULL/DR         0:00:33    192.168.48.189 POS 0/3/0/3
    Neighbor is up for 18:45:27
```

Table 83 describes the significant fields shown in the display.

Table 83 show ospf neighbor Field Descriptions

Field	Description
Neighbor ID	Neighbor router ID.
Pri	Designated router priority.
State	OSPF state.
Dead time	Time (in hh:mm:ss) to elapse before OSPF declares the neighbor dead.
Address	Address of next hop.
Interface	Interface name of next hop.
Neighbor is up	Amount of time (in hh:mm:ss) that the OSPF neighbor has been up.

R3.3 Beta Draft—Cisco Confidential Information

The following is sample output showing summary information about the neighbor that matches the neighbor ID:

```
RP/0/RP0/CPU0:router# show ospf neighbor 192.168.199.137
```

```
Neighbor 192.168.199.137, interface address 172.31.80.37
  In the area 0.0.0.0 via interface POS 0/3/0/2
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 0.0.0.0 BDR is 0.0.0.0
  Options is 0x2
  Dead timer due in 0:00:32
  Neighbor is up for 18:45:30
  Number of DBD retrans during last exchange 0
  Index 1/1, retransmission queue length 0, number of retransmission 0
  First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
  Last retransmission scan length is 0, maximum is 0
  Last retransmission scan time is 0 msec, maximum 0 msec
Neighbor 192.168.199.137, interface address 192.168.48.189
  In the area 0.0.0.0 via interface POS 0/3/0/3
  Neighbor priority is 5, State is FULL, 6 state changes
  Options is 0x2
  Dead timer due in 0:00:32
  Neighbor is up for 18:45:30
  Number of DBD retrans during last exchange 0
  Index 1/1, retransmission queue length 0, number of retransmission 0
  First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
  Last retransmission scan length is 0, maximum is 0
  Last retransmission scan time is 0 msec, maximum 0 msec
```

Total neighbor count: 2

Table 84 describes the significant fields shown in the display.

Table 84 *show ospf neighbor 192.168.199.137 Field Descriptions*

Field	Description
Neighbor	Neighbor router ID.
interface address	IP address of the interface.
In the area	Area and interface through which the OSPF neighbor is known.
Neighbor priority	Router priority of neighbor and neighbor state.
State	OSPF state.
state changes	Number of state changes for this neighbor.
DR is	Neighbor ID of the designated router.
BDR is	Neighbor ID of the backup designated router.
Options	Hello packet options field contents (E-bit only; possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub).
Dead timer	Time (in hh:mm:ss) to elapse before OSPF declares the neighbor dead.
Neighbor is up	Amount of time (in hh:mm:ss) that the OSPF neighbor has been up.
Number of DBD retrans	Number of re-sent database description packets.
Index	Index and the remaining lines of this command give detailed information about flooding information received from the neighbor.

R3.3 Beta Draft—Cisco Confidential Information

If you specify the interface along with the neighbor ID, the software displays the neighbors that match the neighbor ID on the interface, as in the following sample display:

```
RP/0/RP0/CPU0:router# show ospf neighbor POS 0/3/0/2 192.168.199.137

Neighbor 192.168.199.137, interface address 172.31.80.37
  In the area 0.0.0.0 via interface POS 0/3/0/2
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 0.0.0.0 BDR is 0.0.0.0
  Options is 0x2
  Dead timer due in 0:00:32
  Neighbor is up for 18:45:30
  Number of DBD retrans during last exchange 0
  Index 1/1, retransmission queue length 0, number of retransmission 0
  First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
  Last retransmission scan length is 0, maximum is 0
  Last retransmission scan time is 0 msec, maximum 0 msec

Total neighbor count: 1
```

Table 85 describes the significant fields shown in the display.

Table 85 *show ospf neighbor POS 0/3/0/2 192.168.199.137 Field Descriptions*

Field	Description
Neighbor	Neighbor router ID.
interface address	IP address of the interface.
In the area	Area and interface through which the OSPF neighbor is known.
Neighbor priority	Router priority of the neighbor.
State	OSPF state.
state changes	Number of state changes for this neighbor.
DR is	Neighbor ID of the designated router.
BDR is	Neighbor ID of the backup designated router.
Options	Hello packet options field contents (E-bit only; possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub).
Dead timer	Time (in hh:mm:ss) to elapse before OSPF declares the neighbor dead.
Neighbor is up	Amount of time (in hh:mm:ss) that the OSPF neighbor has been up.
Number of DBD retrans	Number of re-sent database description packets.
Index	Index and the remaining lines of this command give detailed information about flooding information received from the neighbor.

You can also specify the interface without the neighbor ID to show all neighbors on the specified interface, as in the following sample display:

```
RP/0/RP0/CPU0:router# show ospf neighbor POS 0/3/0/3

Neighbors for OSPF ospf1

  ID          Pri   State          Dead Time   Address      Interface
192.168.48.1  1    FULL/DROTHER  0:00:33    192.168.48.1  POS 0/3/0/3
  Neighbor is up for 18:50:52
192.168.48.200 1    FULL/DROTHER  0:00:32    192.168.48.200 POS 0/3/0/3
```


R3.3 Beta Draft—Cisco Confidential Information

```
Neighbor is up for 18:50:52
192.168.199.137 5 FULL/DR 0:00:32 192.168.48.189 POS 0/3/0/3
Neighbor is up for 18:50:52
```

Total neighbor count: 3

Table 86 describes the significant fields shown in the display.

Table 86 *show ospf neighbor POS 0/3/0/3 Field Descriptions*

Field	Description
ID	Neighbor router ID.
Pri	Route priority of the neighbor.
State	OSPF state.
Dead Time	Time (in hh:mm:ss) to elapse before OSPF declares the neighbor dead.
Address	Address of next hop.
Interface	Interface name of next hop.
Neighbor is up	Time (in hh:mm:ss) that the OSPF neighbor has been up.
Options	Hello packet options field contents (E-bit only; possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub).
Dead timer	Time (in hh:mm:ss) to elapse before OSPF declares the neighbor dead.
Neighbor is up	Amount of time (in hh:mm:ss) that the OSPF neighbor has been up.
Number of DBD retrans	Number of re-sent database description packets.
Index	Index and the remaining lines of this command give detailed information about flooding information received from the neighbor.

The following is sample output from the **show ospf neighbor detail** command:

```
RP/0/RP0/CPU0:router# show ospf neighbor detail
```

```
Neighbor 192.168.199.137, interface address 172.31.80.37
In the area 0.0.0.0 via interface POS 0/3/0/2
Neighbor priority is 1, State is FULL, 6 state changes
DR is 0.0.0.0 BDR is 0.0.0.0
Options is 0x2
Dead timer due in 0:00:32
Neighbor is up for 18:45:30
Number of DBD retrans during last exchange 0
Index 1/1, retransmission queue length 0, number of retransmission 0
First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
Last retransmission scan length is 0, maximum is 0
Last retransmission scan time is 0 msec, maximum 0 msec
```

Total neighbor count: 1

Table 87 describes the significant fields shown in the display.

R3.3 Beta Draft – Cisco Confidential Information

Table 87 *show ospf neighbor detail Field Descriptions*

Field	Description
Neighbor	Neighbor router ID.
interface address	IP address of the interface.
In the area	Area and interface through which the OSPF neighbor is known.
Neighbor priority	Router priority of neighbor and neighbor state.
State	OSPF state.
state changes	Number of state changes for this neighbor.
DR is	Neighbor ID of the designated router.
BDR is	Neighbor ID of the backup designated router.
Options	Hello packet options field contents (E-bit only; possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub).
Dead timer	Time (in hh:mm:ss) to elapse before OSPF declares the neighbor dead.
Neighbor is up	Amount of time (in hh:mm:ss) that the OSPF neighbor has been up.
Number of DBD retrans	Number of re-sent database description packets.
Index	Index and the remaining lines of this command give detailed information about flooding information received from the neighbor.

Related Commands

Command	Description
router ospf	Configures an OSPF routing process.

R3.3 Beta Draft—Cisco Confidential Information

show ospf request-list

To display the first ten link-state requests pending that the local router is making to the specified Open Shortest Path First (OSPF) neighbor and interface, use the **show ospf request-list** command in EXEC mode.

```
show ospf [process-name] [vrf vrf-name] [area-id] request-list [interface-type interface-instance] [neighbor-id]
```

Syntax Description	
<i>process-name</i>	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the router ospf command. If this argument is included, only information for the specified routing process is displayed.
vrf <i>vrf-name</i>	(Optional) Identifier of an OSPF VPN Routing and Forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as an arbitrary string. The strings 'default' and 'all' are reserved <i>vrf-names</i> .
<i>area-id</i>	(Optional) Area ID. If you do not specify an area, all areas are displayed.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
<i>neighbor-id</i>	(Optional) IP address of the OSPF neighbor.

Defaults	All neighbors

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You might use this command when the databases of two neighboring routers are out of synchronization or if the adjacency does not form between them. Adjacency means that the routers synchronize their databases when they discover each other.

You can look at the list to determine if one router is trying to request a particular database update. Entries that appear to be suspended in the list usually indicate that updates are not being delivered. One possible reason for this behavior is a maximum transmission unit (MTU) mismatch between the routers.

You might also look at this list to make sure it is not corrupted. The list should refer to database entries that actually exist.

Request list information is transient and normally the lists are empty.

Task ID

Task ID	Operations
ospf	Read

Examples

The following is sample output from the **show ospf request-list** command:

```
RP/0/RP0/CPU0:router# show ospf request-list 10.0.124.4 POS3/0/0/0
```

Request Lists for OSPF pagent

Neighbor 10.0.124.4, interface POS3/0/0/0 address 10.3.1.2

Type	LS ID	ADV RTR	Seq NO	Age	Checksum
1	192.168.58.17	192.168.58.17	0x80000012	12	0x0036f3
2	192.168.58.68	192.168.58.17	0x80000012	12	0x00083f

[Table 88](#) describes the significant fields shown in the display.

Table 88 *show ospf request-list 10.0.124.4 POS3/0/0/0 Field Descriptions*

Field	Description
Neighbor	Specific neighbor receiving the request list from the local router.
Interface	Specific interface over which the request list is being sent.
Address	Address of the interface over which the request list is being sent.
Type	Type of link-state advertisement (LSA).
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of the advertising router.
Seq NO	Sequence number of the LSA.
Age	Age of the LSA (in seconds).
Checksum	Checksum of the LSA.

R3.3 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	router ospf	Configures an OSPF routing process.
	show ospf	Displays the first ten link-state entries in the retransmission list that the local router sends to the specified neighbor over the specified interface.
	retransmission-list	

R3.3 Beta Draft—Cisco Confidential Information

show ospf retransmission-list

To display the first ten link-state entries in the Open Shortest Path First (OSPF) retransmission list that the local router sends to the specified neighbor over the specified interface, use the **show ospf retransmission-list** command in EXEC mode.

```
show ospf [process-name] [vrf vrf-name] [area-id] retransmission-list [interface-type
interface-instance] [neighbor-id]
```

Syntax Description

<i>process-name</i>	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the router ospf command. If this argument is included, only information for the specified routing process is displayed.
vrf <i>vrf-name</i>	(Optional) Identifier of an OSPF VPN Routing and Forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as an arbitrary string. The strings 'default' and 'all' are reserved <i>vrf-names</i> .
<i>area-id</i>	(Optional) Area ID. If you do not specify an area, all areas are displayed.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
<i>neighbor-id</i>	(Optional) IP address of the OSPF neighbor.

Defaults

All neighbors

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You might use this command when the databases of two neighboring routers are out of synchronization or if the adjacency is not forming between them. Adjacency means that the routers synchronize their databases when they discover each other.

You can look at the list to determine if one router is trying to request a particular database update. Entries that appear to be suspended in the list usually indicate that updates are not being delivered. One possible reason for this behavior is a maximum transmission unit (MTU) mismatch between the routers.

You might also look at this list to make sure it is not corrupted. The list should refer to database entries that actually exist.

Retransmission list information is transient and normally the lists are empty.

Task ID

Task ID	Operations
ospf	Read

Examples

The following is sample output from the **show ospf retransmission-list** command:

```
RP/0/RP0/CPU0:router# show ospf retransmission-list 10.0.124.4 POS3/0/0/0
```

```
Neighbor 10.0.124.4, interface POS3/0/0/0 address 10.3.1.2
```

Table 89 describes the significant fields shown in the display.

Table 89 show ospf retransmission-list 10.0.124.4 POS3/0/0/0 Field Descriptions

Field	Description
Neighbor	Specified neighbor receiving the retransmission list from the local router.
Interface	Specified interface over which the retransmission list is being sent.
Address	Address of the interface.

Related Commands

Command	Description
router ospf	Configures an OSPF routing process.
show ospf request-list	Displays the first ten link-state requests pending that the local router is making to the specified neighbor and interface.

R3.3 Beta Draft—Cisco Confidential Information

show ospf route

To display the Open Shortest Path First (OSPF) topology table, use the **show ospf route** command in EXEC mode.

```
show ospf [process-name] [vrf vrf-name] route [connected | external | local] [prefix mask]
[prefix/length]
```

Syntax Description	
<i>process-name</i>	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the router ospf command. If this argument is included, only information for the specified routing process is displayed.
vrf <i>vrf-name</i>	(Optional) Identifier of an OSPF VPN Routing and Forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as an arbitrary string. The strings 'default' and 'all' are reserved <i>vrf-names</i> .
connected	(Optional) Displays connected routes.
external	(Optional) Displays routes redistributed from other protocols.
local	(Optional) Displays the local routes redistributed from the Routing Information Base (RIB).
<i>prefix</i>	(Optional) IP prefix, which limits output to a specific route. If the <i>prefix</i> argument is specified, either the <i>length</i> or <i>mask</i> argument is required.
<i>mask</i>	(Optional) IP address mask.
<i>length</i>	(Optional) Prefix length, which can be indicated as a slash (/) and number. For example, /8 indicates that the first eight bits in the IP prefix are network bits. If <i>length</i> is used, the slash is required.

Defaults	All route types

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information

Use the **show ospf route** command to display the OSPF private routing table (which contains only routes calculated by OSPF). If there is something wrong with a route in the RIB, then it is useful to check the OSPF copy of the route to determine if it matches the RIB contents. If it does not match, there is a synchronization problem between OSPF and the RIB. If the routes match and the route is incorrect, OSPF has made an error in its routing calculation.

Task ID

Task ID Operations

ospf	Read

Examples

The following is sample output from the **show ospf route** command:

```
RP/0/RP0/CPU0:router# show ospf route
```

```
Topology Table for ospf 1 with ID 10.3.4.2
```

```
Codes:O - Intra area, O IA - Inter area
```

```
      O E1 - External type 1, O E2 - External type 2
```

```
      O N1 - NSSA external type 1, O N2 - NSSA external type 2
```

```
O E2 10.3.1.0/24, metric 1
      10.3.4.1, from 172.16.10.1, via POS 0/1/0/1
O    10.3.4.0/24, metric 1562
      10.3.4.2, directly connected, via POS 0/1/0/1
O E2 10.1.0.0/16, metric 1
      10.3.4.1, from 172.16.10.1, via POS 0/1/0/1
O IA 10.10.10.0/24, metric 1572
      10.3.4.1, from 172.16.10.1, via POS 0/1/0/1
O E2 130.10.10.0/24, metric 20
      10.3.4.1, from 172.16.10.1, via POS 0/1/0/1
```

[Table 90](#) describes the significant fields shown in the display.

Table 90 *show ospf route Field Descriptions*

Field	Description
O	Network 10.3.1.0 is intra-area.
E2	Interface from which to reach network 10.3.1.0.
10.3.1.0/24	Network and subnet mask to which the local router has a route.
metric 1	Number of hops to network 10.3.1.0.
10.3.4.1	Next-hop router on the path to network 10.3.1.0.
from 172.16.10.1	Router ID 172.16.10.1 is the router that advertised this route.
via POS 0/1/0/1	Packets destined for the given prefix (10.3.1.0/24) are sent over POS interface 0/1/0/1.

The following is sample output from the **show ospf route** command with a process name of 100:

```
RP/0/RP0/CPU0:router# show ospf 100 route
```

```
Topology Table for ospf 100 with ID 172.23.54.14
```

```
Codes:O - Intra area, O IA - Inter area
```

```
      O E1 - External type 1, O E2 - External type 2
```

R3.3 Beta Draft—Cisco Confidential Information

```

O N1 - NSSA external type 1, O N2 - NSSA external type 2

O 10.1.5.0/24, metric 1562
    10.1.5.14, directly connected, via POS 0/3/0/3
O IA 21.0.0.0/24, metric 1572
    10.1.5.12, from 172.23.54.12, via POS 0/3/0/3
O 10.0.0.0/24, metric 10
    10.0.0.12, directly connected, via POS 0/2/0/3

```

Table 91 describes the significant fields shown in the display.

Table 91 *show ospf 100 route Field Descriptions*

Field	Description
O	Network 10.3.1.0 is intra-area.
IA	Interface from which to reach network 10.1.5.0.
10.1.5.0/24	Network and subnet mask to which the local router has a route.
metric 1562	Cost to reach network 10.1.5.0.
10.1.5.14	Next-hop router on the path to network 10.1.5.0.
from 172.23.54.12	Router ID 172.23.54.12 is the router that advertised this route.
via POS 0/3/0/3	Packets destined for the given prefix (10.3.1.0/24) are sent over POS interface 0/3/0/3.

The following is sample output from the **show ospf route** command with a prefix of 10.0.0.0 and a length of 24:

```

RP/0/RP0/CPU0:router# show ospf route 10.0.0.0/24

Topology Table for ospf 100 with ID 172.23.54.14

Codes:O - Intra area, O IA - Inter area
       O E1 - External type 1, O E2 - External type 2
       O N1 - NSSA external type 1, O N2 - NSSA external type 2

O IA 10.0.0.0/24, metric 1572
    10.1.5.12, from 172.23.54.12, via POS 0/3/0/3

```

Table 92 describes the significant fields shown in the display.

Table 92 *show ospf route 10.0.0.0/24 Field Descriptions*

Field	Description
O	Route is an OSPF route.
IA	Route to network 10.0.0.0 is an interarea route.
10.0.0.0/24	Network and subnet mask to which the local router has a route.
metric 1572	Cost to reach network 10.0.0.0.
10.1.5.12	IP address of next-hop router on the path to network 10.0.0.0.
from 172.23.54.12	Router ID 172.23.54.12 is the router that advertised this route.
via POS 0/3/0/3	Packets destined for the given prefix (10.0.0.0/24) are sent over POS interface 0/3/0/3.

R3.3 Beta Draft—Cisco Confidential Information**Related Commands**

Command	Description
router ospf	Configures an OSPF routing process.

R3.3 Beta Draft—Cisco Confidential Information

show ospf summary-prefix

To display Open Shortest Path First (OSPF) aggregated summary address information, use the **show ospf summary-prefix** command in EXEC mode.

show ospf [*process-name*] [*vrf vrf-name*] **summary-prefix**

Syntax Description

<i>process-name</i>	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the router ospf command. If this argument is included, only information for the specified routing process is displayed.
vrf <i>vrf-name</i>	(Optional) Identifier of an OSPF VPN Routing and Forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as an arbitrary string. The strings 'default' and 'all' are reserved <i>vrf-names</i> .

Defaults

All summary prefixes

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show ospf summary-prefix** command if you configured summarization of external routes with the **summary-prefix** command and you want to display configured summary addresses.

Task ID

Task ID	Operations
ospf	Read

Examples

The following is sample output from the **show ospf summary-prefix** command:

```
RP/0/RP0/CPU0:router# show ospf summary-prefix
```

```
OSPF Process 1, summary-prefix
```

```
10.1.0.0/255.255.0.0 Metric 20, Type 2, Tag 0
```

R3.3 Beta Draft—Cisco Confidential Information

Table 93 describes the significant fields shown in the display.

Table 93 *show ospf summary-prefix Field Descriptions*

Field	Description
10.1.0.0/255.255.0.0	Summary address designated for a range of addresses. The IP subnet mask used for the summary route.
Metric	Metric used to advertise the summary routes.
Type	External link-state advertisements (LSA) metric type.
Tag	Tag value that can be used as a “match” value for controlling redistribution through route maps.

Related Commands

Command	Description
router ospf	Configures an OSPF routing process.
summary-prefix (OSPF)	Creates aggregate addresses for routes being redistributed from another routing protocol into the OSPF protocol.

R3.3 Beta Draft – Cisco Confidential Information

show ospf virtual-links

To display parameters and the current state of Open Shortest Path First (OSPF) virtual links, use the **show ospf virtual-links** command in EXEC mode.

```
show ospf [process-name] [vrf vrf-name] virtual-links
```

Syntax Description	<i>process-name</i>	(Optional) Name that uniquely identifies an OSPF routing process. The process name is defined by the router ospf command. If this argument is included, only information for the specified routing process is displayed.
	vrf <i>vrf-name</i>	(Optional) Identifier of an OSPF VPN Routing and Forwarding (VRF) instance. The <i>vrf-name</i> argument can be specified as an arbitrary string. The strings ‘default’ and ‘all’ are reserved <i>vrf-names</i> .

Defaults	All virtual links

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the show ospf virtual-links command to display useful information for debugging OSPF routing operations.

Task ID	Task ID	Operations
	ospf	Read

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following is sample output from the **show ospf virtual-links** command:

```
RP/0/RP0/CPU0:router# show ospf virtual-links
```

```
Virtual Link to router 172.31.101.2 is up
Transit area 0.0.0.1, via interface POS 0/3/0/0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

Table 94 describes the significant fields shown in the display.

Table 94 *show ospf virtual-links Field Descriptions*

Field	Description
Virtual Link to router 172.31.101.2 is up	OSPF neighbor and whether the link to that neighbor is up or down.
Transit area 0.0.0.1	Transit area through which the virtual link is formed.
via interface POS 0/3/0/0	Interface through which the virtual link is formed.
Cost of using 10	Cost of reaching the OSPF neighbor through the virtual link.
Transmit Delay is 1 sec	Transmit delay (in seconds) on the virtual link.
State POINT_TO_POINT	State of the OSPF neighbor.
Timer intervals	Various timer intervals (in seconds) configured for the link.
Hello due in 0:00:08	When the next hello message is expected from the neighbor (in hh:mm:ss).
Adjacency State FULL	Adjacency state between the neighbors.

Related Commands

Command	Description
router ospf	Configures an OSPF routing process.

R3.3 Beta Draft – Cisco Confidential Information

show protocols (OSPF)

To display information about the OSPFv2 processes running on the router, use the **show protocols** command in EXEC mode.

```
show protocols [afi-all | ipv4 | ipv6] [all | protocol]
```

Syntax Description	afi-all	(Optional) Specifies all address families.
	ipv4	(Optional) Specifies an IPv4 address family.
	ipv6	(Optional) Specifies an IPv6 address family.
	all	(Optional) Specifies all protocols for a given address family.
	protocol	(Optional) Specifies a routing protocol. For the IPv4 address family, the options are: • bgp • isis • ospf For the IPv6 address family, the options are: • bgp • isis • ospfv3

Defaults No default behavior or value

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The afi-all keyword was added.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	ospf	Read
	rib	Read

Examples

The following is an OSPF configuration and the resulting **show protocols ospf** display:

```
RP/0/RP0/CPU0:router# show running router ospf 1
```

```
router ospf 1
router-id Loopback0
nsf
redistribute connected
redistribute isis 3
area 0
interface Loopback0
!
interface Loopback1
!
interface Loopback2
!
interface POS 0/3/0/0
!
interface POS 0/3/0/1
!
interface POS 0/3/0/2
!
interface POS 0/3/0/3
!
!
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
!
```

```
RP/0/RP0/CPU0:router# show protocols ospf
```

```
Routing Protocol OSPF 1
Router Id: 55.55.55.55
Distance: 110
Non-Stop Forwarding: Enabled
Redistribution:
connected
isis 3
Area 0
MPLS/TE enabled
POS 0/3/0/3
POS 0/3/0/2
POS 0/3/0/1
POS 0/3/0/0
Loopback2
Loopback0
```

Table 95 describes the significant fields shown in the display.

R3.3 Beta Draft – Cisco Confidential Information

Table 95 *show protocols ospf Field Descriptions*

Field	Description
Router Id	ID of the router for this configuration.
Distance	Administrative distance of OSPF routes relative to routes from other protocols.
Non-Stop Forwarding	Status of nonstop forwarding.
Redistribution	Lists the protocols that are being redistributed.
Area	Information about the current area including list of interfaces and the status of Multiprotocol Label Switching traffic engineering (MPLS TE).

R3.3 Beta Draft—Cisco Confidential Information

stub (OSPF)

To define an area as a stub area, use the **stub** command in area configuration mode. To disable this function, use the **no** form of this command.

stub [**no-summary**]

no stub

Syntax Description	no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.

Defaults	No stub area is defined.

Command Modes	Area configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

You must configure the **stub** command on all routers in the stub area. Use the **default-cost** command to specify the cost of a default internal router sent into a stub area by an ABR.

Two stub area router configuration commands exist: the **stub** and **default-cost** commands. In all routers attached to the stub area, the area should be configured as a stub area using the **stub** command. Use the **default-cost** command only on an ABR attached to the stub area. Use the **default cost** command on the ABR of a stub area to specify the cost of the default route advertised into the stub area by the ABR.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the **no-summary** keyword on the ABR to prevent it from sending summary LSAs (LSA Type 3) into the stub area.

Task ID	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to assign a default cost of 20 to stub network 10.0.0.0:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 201
RP/0/RP0/CPU0:router(config-ospf)# area 10.0.0.0
RP/0/RP0/CPU0:router(config-ospf-ar)# stub
RP/0/RP0/CPU0:router(config-ospf-ar)# default-cost 20
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/3/0/3
```

Related Commands

Command	Description
authentication (OSPF)	Enables authentication for an OSPF area.
default-cost (OSPF)	Specifies a cost for the default summary route sent into a stub area.

R3.3 Beta Draft—Cisco Confidential Information

summary-prefix (OSPF)

To create aggregate addresses for routes being redistributed from another routing protocol into the Open Shortest Path First (OSPF) protocol, use the **summary-prefix** command in router configuration mode. To stop summarizing redistributed routes, use the **no** form of the command.

summary-prefix *address mask* [**not-advertise** | **tag** *tag*]

no summary-prefix *address mask*

Syntax Description

<i>address</i>	Summary address designated for a range of addresses.
<i>mask</i>	IP subnet mask used for the summary route.
not-advertise	(Optional) Suppresses summary routes that match the address and mask pair from being advertised.
tag <i>tag</i>	(Optional) Tag value that can be used as a “match” value for controlling redistribution through route maps.

Defaults

When this command is not used in router configuration mode, aggregate addresses are not created for routes being redistributed from another routing protocol into the OSPF protocol.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **summary-prefix** command to cause an OSPF Autonomous System Boundary Router (ASBR) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. This command summarizes only routes from other routing protocols that are being redistributed into OSPF.

You can use this command multiple times to summarize multiple groups of addresses. The metric used to advertise the summary is the lowest metric of all the more specific routes. This command helps reduce the size of the routing table.

If you want to summarize routes between OSPF areas, use the **range** command.

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	ospf	read, write

Examples

In the following example, summary address 10.1.0.0 includes address 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. Only the address 10.1.0.0 is advertised in an external link-state advertisement.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 201
RP/0/RP0/CPU0:router(config-ospf)# summary-prefix 10.1.0.0 255.255.0.0
```

Related Commands	Command	Description
	range (OSPF)	Consolidates and summarizes routes at an area boundary.

R3.3 Beta Draft—Cisco Confidential Information

timers lsa group-pacing

To change the interval at which Open Shortest Path First (OSPF) link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers lsa group-pacing** command in router configuration mode. To restore the default value, use the **no** form of this command.

timers lsa group-pacing *seconds*

no timers lsa group-pacing

Syntax Description	<i>seconds</i>	Interval (in seconds) at which LSAs are grouped and refreshed, checksummed, or aged. Range is 10 seconds to 1800 seconds.

Defaults	<i>seconds</i> : 240 seconds

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

OSPF LSA group pacing is enabled by default. For typical customers, the default group pacing interval for refreshing, checksumming, and aging is appropriate and you need not configure this feature.

The duration of the LSA group pacing is inversely proportional to the number of LSAs the router is handling. For example, if you have approximately 10,000 LSAs, decreasing the pacing interval would benefit you. If you have a very small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might benefit you slightly.

Task ID.	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to change the OSPF pacing between LSA groups to 60 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# timers lsa group-pacing 60
```


R3.3 Beta Draft—Cisco Confidential Information

timers lsa min-arrival

To limit the frequency that new instances of any particular Open Shortest Path First (OSPF) link-state advertisements (LSAs) can be accepted during flooding, use the **timers lsa min-arrival** command in router configuration mode. To restore the default value, use the **no** form of this command.

timers lsa min-arrival *seconds*

no timers lsa min-arrival

Syntax Description	<i>seconds</i>	Minimum interval (in seconds) between instances of the same LSA. Range is 0 to 1800 seconds.

Defaults	<i>seconds</i> : 1 second

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	ospf	read, write

Examples	The following example shows how to change the minimum interval between accepting the same LSA to 2 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# timers lsa min-arrival 2
```

R3.3 Beta Draft—Cisco Confidential Information**timers throttle lsa all (OSPF)**

To turn on Open Shortest Path First (OSPF) link-state advertisement (LSA) throttling, use the **timers throttle lsa all** command in router configuration mode. To turn off LSA throttling, use the **no** form of this command

timers throttle lsa all *lsa-start lsa-hold lsa-max-wait*

no timers throttle lsa all *lsa-start lsa-hold lsa-max-wait*

Syntax Description	<i>lsa-start</i>	Initial LSA schedule delay (in milliseconds). Range is 1 to 600000 milliseconds.
	<i>lsa-hold</i>	Minimum hold time (in milliseconds) between two consecutive LSA calculations. Range is 1 to 600000 milliseconds.
	<i>lsa-max-wait</i>	Maximum wait time (in milliseconds) between two consecutive LSA calculations. Range is 1 to 600000 milliseconds.

Defaults LSA throttling is not set.

Command Modes Router configuration
VRF configuration

Command History	Release	Modification
	Release 3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
	Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The *lsa-start* time is the delay before flooding the first instance of an LSA. The *lsa-hold* interval is the minimum time to elapse before flooding an updated instance of an LSA. The *lsa-max-wait* time is the maximum time that can elapse before flooding an updated instance of an LSA.

For quick convergence, use smaller times for the *lsa-start* time and *lsa-hold* interval. However, in relatively large networks, this may result in a large number of LSAs being flooded in a relatively short time. A balance with the *lsa-start* time and *lsa-hold* interval can be iteratively arrived at for the size of your network. The *lsa-max-wait* time can be used to ensure that OSPF reconverges within a reasonable amount of time.

Task ID	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to change the start, hold, and maximum wait interval values to 5, 1000, and 90,000 milliseconds, respectively:

```
RP/0/RP0/CPU0:router# configure  
RP/0/RP0/CPU0:router(config)# router ospf 1  
RP/0/RP0/CPU0:router(config-ospf)# timers throttle lsa all 5 1000 90000
```

R3.3 Beta Draft—Cisco Confidential Information

timers throttle spf (OSPF)

To turn on Open Shortest Path First (OSPF) shortest path first (SPF) throttling, use the **timers throttle spf** command in router configuration mode. To turn off SPF throttling, use the **no** form of this command

```
timers throttle spf spf-start spf-hold spf-max-wait

no timers throttle spf spf-start spf-hold spf-max-wait
```

Syntax Description	<i>spf-start</i>	Initial SPF schedule delay (in milliseconds). Range is 1 to 600000 milliseconds.
	<i>spf-hold</i>	Minimum hold time (in milliseconds) between two consecutive SPF calculations. Range is 1 to 600000 milliseconds.
	<i>spf-max-wait</i>	Maximum wait time (in milliseconds) between two consecutive SPF calculations. Range is 1 to 600000 milliseconds.

Defaults SPF throttling is not set.

Command Modes Router configuration
VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The *spf-start* time is the delay before running SPF for the first time. The *spf-hold* interval is the minimum time to elapse between subsequent SPF runs. The *spf-max-wait* time is the maximum time that can elapse before running SPF again.



Tip Setting a low *spf-start* time and *spf-hold* time causes routing to switch to the alternate path more quickly if there is a failure. However, it consumes more CPU processing time.

Task ID	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to change the start, hold, and maximum wait interval values to 5, 1000, and 90000 milliseconds, respectively:

```
RP/0/RP0/CPU0:router# configure  
RP/0/RP0/CPU0:router(config)# router ospf 1  
RP/0/RP0/CPU0:router(config-ospf)# timers throttle spf 5 1000 90000
```

R3.3 Beta Draft—Cisco Confidential Information

transmit-delay (OSPF)

To set the estimated time required to send a link-state update packet on the interface, use the **transmit-delay** command. To return to the default value, use the **no** form of this command.

transmit-delay *seconds*

no transmit-delay *seconds*

Syntax Description	<i>seconds</i>	Time (in seconds) required to send a link-state update. Range is 1 to 65535 seconds.

Defaults	<i>seconds</i> : 1 second

Command Modes	Router configuration Area configuration Interface configuration Virtual-link configuration VRF configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	This command was added under the VRF configuration mode.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the *seconds* argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, this means that the time in which the LSA propagates over the link is not considered. This setting has more significance on very low speed links and can result in more LSA transmissions during the maximum aging of LSAs when there is significant time required between an LSA being transmitted and received by the target neighbors.

Task ID	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure a transmit delay for Packet-over-SONET/SDH (POS) interface POS 0/3/0/0:

```
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# interface POS 0/3/0/0
RP/0/RP0/CPU0:router(config-ospf-ar-if)# transmit-delay 3
```

Related Commands

Command	Description
show ospf	Displays general information about OSPF routing processes.
virtual-link (OSPF)	Sets the estimated time required to send a link-state update packet on the interface.

R3.3 Beta Draft—Cisco Confidential Information

virtual-link (OSPF)

To define an Open Shortest Path First (OSPF) virtual link, use the **virtual-link** command in area configuration mode with the optional parameters. To remove a virtual link, use the **no** form of this command.

virtual-link *router-id*

no virtual-link *router-id*

Syntax Description

<i>router-id</i>	Router ID associated with the virtual link neighbor. The router ID appears in the show ospf command display. The <i>router-id</i> can be any 32-bit router ID value specified in four-part, dotted-decimal notation.

Defaults

No virtual links are defined.

Command Modes

Area configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

All areas in an OSPF autonomous system must be physically connected to the backbone area (area 0). In some cases in which this physical connection is not possible, you can use a virtual link to connect to the backbone through a nonbackbone area. You can also use virtual links to connect two parts of a partitioned backbone through a nonbackbone area. The area through which you configure the virtual link, known as a transit area, must have full routing information. The transit area cannot be a stub area.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to establish a virtual link with default values for all optional parameters:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 201
```


R3.3 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config-ospf)# area 10.0.0.0
RP/0/RP0/CPU0:router(config-ospf-ar)# virtual-link 10.3.4.5
RP/0/RP0/CPU0:router(config-ospf-ar-vl)# interface POS0/3/0/0
```

The following example shows how to establish a virtual link with clear text authentication called mykey:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf 201
RP/0/RP0/CPU0:router(config-ospf)# area 10.0.0.0
RP/0/RP0/CPU0:router(config-ospf-ar)# virtual-link 10.3.4.5
RP/0/RP0/CPU0:router(config-ospf-ar-vl)# authentication-key 0 mykey
```

Related Commands

Command	Description
authentication (OSPF)	Enables authentication for an OSPF area.
show ospf virtual-links	Displays parameters and the current state of OSPF virtual links

R3.3 Beta Draft – Cisco Confidential Information

vrf (OSPF)

To configure an Open Shortest Path First (OSPF) VPN Routing and Forwarding (VRF) instance, use the **vrf** command in router configuration mode. To terminate an OSPF VRF, use the **no** form of this command.

```
vrf vrf-name

no vrf vrf-name
```

Syntax Description	vrf-name	Identifier of an OSPF VRF. The <i>vrf-name</i> argument can be specified as an arbitrary string. The strings ‘default’ and ‘all’ are reserved <i>vrf-names</i> .

Defaults	No OSPF VRF is defined.

Command Modes	Router configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and the Cisco XR 12000 Series Router

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **vrf** command to explicitly configure a VRF. Commands configured under the VRF configuration mode (such as the **interface** [OSPF] and **authentication** commands) are automatically bound to that vrf.

To modify or remove the VRF, the *vrf-id* argument format must be the same as the format used when creating the area.



Note

To remove the specified area from the router configuration, use the **no vrf vrf-id** command. The **no vrf vrf-id** command removes the VRF and all VRF options, such as **authentication**, **default-cost**, **nssa**, **range**, **stub**, **virtual-link**, and **interface**.

Task ID	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure VRF vrf1 and Packet-over-SONET/SDH (POS) interface 0/2/0/0. POS interface 0/2/0/0 is bound to VRF vrf1 automatically.

```
RP/0/RP0/CPU0:router# configure  
RP/0/RP0/CPU0:router(config)# router ospf 1  
RP/0/RP0/CPU0:router(config-ospf)# vrf vrf1  
RP/0/RP0/CPU0:router(config-ospf-vrf)# interface POS 0/2/0/0
```

R3.3 Beta Draft – Cisco Confidential Information

OSPFv3 Commands on Cisco IOX XR Software

Beta Draft Highly Confidential Information

This chapter describes the commands used to configure and monitor the IP Version 6 (IPv6) Open Shortest Path First Version 3 (OSPFv3) routing protocol.

For detailed information about OSPFv3 concepts, configuration tasks, and examples, refer to the *Implementing OSPF on Cisco IOS XR Software* configuration guide.

R3.3 Beta Draft—Cisco Confidential Information

address-family (OSPFv3)

To enter address family configuration mode for Open Shortest Path First Version 3 (OSPFv3), use the **address-family** command in the router configuration mode. To disable address family configuration mode, use the **no** form of this command.

address-family ipv6 [unicast]

no address-family ipv6 [unicast]

Syntax Description	ipv6	Specifies IP Version 6 (IPv6) address prefixes.
	unicast	(Optional) Specifies unicast address prefixes.

Defaults	An address family is not specified.

Command Modes	Router ospfv3 configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	At present, OSPFv3 provides routing services only for IPv6 unicast topologies, so this command has no effect.

Task ID	Task ID	Operations
	ospf	read, write

Examples	The following example shows how to configure the OSPFv3 router process with IPv6 unicast address prefixes:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# address-family ipv6 unicast
```

R3.3 Beta Draft—Cisco Confidential Information

area (OSPFv3)

To configure an Open Shortest Path First Version 3 (OSPFv3) area, use the **area** command in router ospfv3 configuration mode. To remove an OSPFv3 area, use the **no** form of this command.

area *area-id*

no area *area-id*

Syntax Description	<i>area-id</i>	Identifier of an OSPFv3 area. The <i>area-id</i> argument can be specified as either a decimal value or as an IPv4 address.

Defaults	No OSPFv3 areas are defined.

Command Modes	Router ospfv3 configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

An area must be explicitly configured with the **area** command.

Use the **area** command to place the router in area configuration mode (prompt: config-router-ar), from which you can configure area-specific settings. Commands configured under this mode (such as the **interface** command) are automatically bound to that area.



Note

To remove the specified OSPFv3 area from the router ospfv3 configuration, use the **no area area-id** command. The **no area area-id** command removes the OSPFv3 area including all OSPFv3 area options, and all the OSPFv3 interfaces and interface options that are configured under the area.

Task ID	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure area 0 for OSPFv3 process 1. The Packet-over-SONET (POS) 0/1/0/1 interface also is configured:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1  
RP/0/RP0/CPU0:router(config-ospfv3)# area 0  
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/1/0/1
```


R3.3 Beta Draft—Cisco Confidential Information

authentication (OSPFv3)

To enable plain text, Message Digest 5 (MD5) authentication, or null authentication for an Open Shortest Path First Version 3 (OSPFv3) interface, use the **authentication** command in the appropriate mode. To remove such authentication, use the **no** form of this command.

authentication {ipsec spi *spi-value* {md5 | sha1} [clear | encrypted] *password* | disable}

no authentication

Syntax Description

ipsec	Specifies IP Security (IPSec).
spi <i>spi-value</i>	Specifies a security policy index (SPI) value. Range is 256 to 4294967295.
md5	Enables Message Digest 5 (MD5) authentication.
sha1	Enables SHA1 authentication.
clear	(Optional) Specifies that the key be unencrypted.
encrypted	(Optional) Specifies that the key be encrypted using a two-way algorithm.
<i>password</i>	Any contiguous string of characters up to 8 bytes in length that can be entered from the keyboard.
disable	Disables authentication for OSPFv3 packets.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the authentication parameter specified by the area.
 If this command is not specified in area configuration mode, then the interface adopts the authentication parameter specified for the process.
 If this command is not specified at any level, then the interface does not use authentication.

Command Modes

Interface configuration
 Area configuration
 Router configuration
 Virtual-link configuration

Command History

Release	Modification
Release 3.2	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft – Cisco Confidential Information

Use the **authentication** command to specify an authentication type for the interface, which overrides the authentication specified for the area to which this interface belongs. If this command is not included in the configuration file, the authentication configured in the area to which the interface belongs is assumed (as specified by the area **authentication** command).

The authentication type and password must be the same for all OSPFv3 interfaces that are to communicate with each other through OSPFv3.

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows how to enable MD5 authentication:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospfv3 201
RP/0/RP0/CPU0:router(config-ospfv3)# router-id 10.1.1.1
RP/0/RP0/CPU0:router(config-ospfv3)# authentication ipsec spi 500 md5
1234567890abcdef1234567890abcdef
```

R3.3 Beta Draft—Cisco Confidential Information

auto-cost (OSPFv3)

To control how the Open Shortest Path First Version 3 (OSPFv3) protocol calculates default metrics for an interface, use the **auto-cost** command in router ospfv3 configuration mode. To set link cost based only on the interface type, use the **disable** form of this command. To re-enable OSPFv3 metric calculation for an interface according to the bandwidth of the interface, use the **no** form of this command.

auto-cost [**reference-bandwidth** *mbps* | **disable**]

no auto-cost [**reference-bandwidth** *mbps* | **disable**]

Syntax Description	reference-bandwidth <i>mbps</i>	(Optional) Sets the rate in Mbps (bandwidth). Range is 1 to 4294967.
	disable	(Optional) Sets the link cost based only on the interface type.

Defaults	<i>mbps</i> : 100 Mbps

Command Modes	Router ospfv3 configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

By default OSPFv3 calculates the OSPFv3 metric for an interface according to the bandwidth of the interface.

The **no auto-cost disable** form of this command reenables OSPFv3 metric calculation for an interface according to the bandwidth of the interface.

To set link cost based only on the interface type, use the **disable** keyword.

If you have multiple links with high bandwidth, you might want to use a larger number to differentiate the cost on those links.

Recommended usage of cost configuration for all OSPFv3 configured interfaces is to be consistent: Either explicitly configure link costs (by using the **cost** command) or choose an appropriate default (by using the **auto-cost** command).

The value set by the **cost** command overrides the cost resulting from the **auto-cost** command.

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows how to set the reference value for the auto cost to 64:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1  
RP/0/RP0/CPU0:router(config-ospfv3)# auto-cost reference-bandwidth 64
```

Related Commands	Command	Description
	cost (OSPFv3)	Explicitly specifies the cost of sending a packet on an interface.

R3.3 Beta Draft—Cisco Confidential Information

clear ospfv3 process

To reset an Open Shortest Path First Version 3 (OSPFv3) router process without removing and reconfiguring it, use the **clear ospfv3 process** command in EXEC mode.

clear ospfv3 [*process-name*] **process**

Syntax Description	<i>process-name</i>	(Optional) Name that uniquely identifies an OSPFv3 routing process. The process name is defined by the router ospfv3 command. If this argument is included, only the specified routing process is affected. Otherwise, all OSPFv3 processes are reset.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. When the OSPFv3 router process is reset, OSPFv3 releases all resources allocated, cleans up the internal database, uninstalls routes, and resets all OSPFv3 adjacencies.

Task ID	Task ID	Operations
	ospf	read, write

Examples	The following example shows how to reset all OSPFv3 processes: <pre>RP/0/RP0/CPU0:router# clear ospfv3 process</pre> The following example shows how to reset the OSPFv3 process 1: <pre>RP/0/RP0/CPU0:router# clear ospfv3 1 process</pre>

R3.3 Beta Draft—Cisco Confidential Information

clear ospfv3 redistribution

To flush all the Type 5 and Type 7 link-state advertisements (LSAs) originated by an Open Shortest Path First Version 3 (OSPFv3) process, use the **clear ospfv3 redistribution** command in EXEC mode.

clear ospfv3 [*process-name*] **redistribution**

Syntax Description	<i>process-name</i>	(Optional) Name that uniquely identifies an OSPFv3 routing process. The process name is defined by the router ospfv3 command. If this argument is included, only the specified routing process is affected. Otherwise, all OSPFv3 processes are reset.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **clear ospfv3 redistribution** command to cause the routing table to be read again. OSPFv3 regenerates and sends Type 5 and Type 7 link-state advertisements (LSAs) to its neighbors. If an unexpected route has appeared in the OSPFv3 redistribution, using this command corrects the issue.

**Note**

Use of this command can cause a significant number of LSAs to flood the network. We recommend that you use this command with caution.

Task ID	Task ID	Operations
	ospf	read, write

Examples	The following example shows how to clear all OSPFv3 redistributed routes from other protocols:

```
RP/0/RP0/CPU0:router# clear ospfv3 redistribution
```

R3.3 Beta Draft—Cisco Confidential Information

clear ospfv3 routes

To clear the Open Shortest Path First Version 3 (OSPFv3) internal route table, use the **clear ospfv3 routes** command in EXEC mode.

clear ospfv3 [*process-name*] **routes**

Syntax Description

<i>process-name</i>	(Optional) Name that uniquely identifies an OSPFv3 routing process. The process name is defined by the router ospfv3 command. If this argument is included, only the specified routing process is affected. Otherwise, all OSPFv3 processes are reset.

Defaults

No default behavior or value

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **clear ospfv3 routes** command to force the internal route table to be repopulated by causing recalculation of the shortest path first (SPF) routing table. When the OSPFv3 routing table is cleared, OSPFv3 routes in the global routing table are also recalculated.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to clear all OSPFv3 routes from the OSPFv3 routing table and recomputes valid routes:

```
RP/0/RP0/CPU0:router# clear ospfv3 routes
```

R3.3 Beta Draft—Cisco Confidential Information

clear ospfv3 statistics

To clear the Open Shortest Path First Version 3 (OSPFv3) statistical counters, use the **clear ospfv3 statistics** command in EXEC mode.

clear ospfv3 [*process-name*] **statistics** [**neighbor** [*interface-type interface-instance*] [*router-id*]]

Syntax Description

<i>process-name</i>	(Optional) Name that uniquely identifies an OSPFv3 routing process. The process name is defined by the router ospfv3 command. If this argument is included, only the specified routing process is affected.
neighbor	(Optional) Clears counters for the specified neighbor only.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a Route Processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
<i>router-id</i>	(Optional) Specified router ID. This argument must be in 32-bit dotted-decimal notation, similar to an IPv4 address. This argument clears the counters of the specified neighbor only.

Defaults

No default behavior or value

Command Modes

EXEC

R3.3 Beta Draft—Cisco Confidential Information

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **clear ospfv3 statistics** command to reset statistics so that subsequent changes are easily observed.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to clear the OSPFv3 statistical counters of all neighbors on Packet-over-SONET (POS) interface 0/2/0/0:

```
RP/0/RP0/CPU0:router# clear ospfv3 statistics neighbor POS 0/2/0/0
```

R3.3 Beta Draft—Cisco Confidential Information**cost (OSPFv3)**

To explicitly specify the cost of sending a packet on an interface for the Open Shortest Path First Version 3 (OSPFv3) router process, use the **cost** command in the appropriate configuration mode. To remove the cost, use the **no** form of this command.

cost *cost*

no *cost*

Syntax Description

<i>cost</i>	Unsigned integer value expressed as the link-state metric. Range is 1 to 65535.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the cost parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the cost parameter specified for the process.

If this command is not specified at any level, then the cost is based on the interface bandwidth, as specified by the **auto-cost** command.

Command Modes

Interface configuration
Area configuration
Router ospfv3 configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The link-state metric is advertised as the link cost in the router link advertisement.

In general, the path cost is calculated using the following formula:

$$10^8 / \text{bandwidth}$$

Using this formula, the default path cost is 1 for OC-3 Packet-over-SONET (POS). If this value does not suit your network, you can use your own method of calculating path costs.

The value set by the **cost** command overrides the cost resulting from the **auto-cost** command.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows how to set the cost value to 65 for Packet-over-SONET (POS) interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 201  
RP/0/RP0/CPU0:router(config-ospfv3)# area 0  
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/1/0/1  
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# cost 65
```

Related Commands

Command	Description
auto-cost (OSPFv3)	Controls how the OSPFv3 protocol calculates default metrics for an interface.

R3.3 Beta Draft—Cisco Confidential Information**database-filter all out (OSPFv3)**

To filter outgoing link-state advertisements (LSAs) to an Open Shortest Path First Version 3 (OSPFv3) interface, use the **database-filter** command in the appropriate command mode. To restore the forwarding of LSAs to the interface, use the **no** form of this command.

database-filter all out

no database-filter all out

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the database filter parameter specified for the area.

If this command is not specified in area configuration mode, then the interface adopts the database filter parameter specified for the process.

If this command is not specified in router ospfv3 configuration mode, then the database filter is disabled and all outgoing LSAs are flooded to the interface.

Command Modes

Interface configuration

Area configuration

Router ospfv3 configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **database-filter all out** command to perform the same function that the **neighbor** command (with the **database-filter** keyword) performs on a neighbor basis.

Task ID

Task ID	Operations
ospf	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to prevent flooding of OSPFv3 LSAs to neighbors reachable through Packet-over-SONET (POS) interface 0/2/0/3:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# area 0
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/2/0/3
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# database-filter all out
```

Related Commands

Command	Description
neighbor (OSPFv3)	Configures OSPFv3 routers interconnecting to nonbroadcast networks.

R3.3 Beta Draft—Cisco Confidential Information

dead-interval (OSPFv3)

To set the interval after which a neighbor is declared dead when no hello packets are observed, use the **dead-interval** command in the appropriate configuration mode. To return to the default time, use the **no** form of this command.

dead-interval *seconds*

no dead-interval

Syntax Description

<i>seconds</i>	Unsigned integer that specifies the interval (in seconds). The value must be the same for all nodes on the same network link. Range is 1 to 65535.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the dead interval parameter specified for the area.

If this command is not specified in area configuration mode, then the interface adopts the dead interval parameter specified for the process.

If this command is not specified in router ospfv3 configuration mode, then the dead interval is four times the interval set by the **hello-interval (OSPFv3)** command.

Command Modes

Interface configuration
Area configuration
Router ospfv3 configuration
Virtual-link configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Two Open Shortest Path First Version 3 (OSPFv3) routers do not become adjacent if their dead interval values differ.

If the hello interval is configured, the dead interval value must be larger than the hello interval value. The dead interval value is usually configured four times larger than the hello interval value.

Task ID

Task ID	Operations
ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to set the OSPFv3 dead interval on Packet-over-SONET (POS) interface 0/2/0/3 to 40 seconds:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# area 0
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/2/0/3
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# dead-interval 40
```

Related Commands

Command	Description
hello-interval (OSPFv3)	Specifies the interval between hello packets that the Cisco IOS XR software sends on the interface.

R3.3 Beta Draft—Cisco Confidential Information

default-cost (OSPFv3)

To specify a cost for the default summary route sent into a stub area or not-so-stubby area (NSSA) for Open Shortest Path First Version 3 (OSPFv3) packets, use the **default-cost** command in area configuration mode. To remove the assigned default route cost, use the **no** form of this command.

default-cost *cost*

no default-cost *cost*

Syntax Description	<i>cost</i>	Cost for the default summary route used for a stub or NSSA area. The acceptable value is a 24-bit number.

Defaults	<i>cost</i> : 1

Command Modes	Area configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **default-cost** command only on an Area Border Router (ABR) attached to a stub or an NSSA area.

In all routers and access servers attached to the stub area, the area should be configured as a stub area using the **stub (OSPFv3)** command in the area configuration submode. Use the **default-cost** command only on an ABR attached to the stub area. The **default-cost** command provides the metric for the summary default route generated by the ABR into the stub area.

Task ID	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to assign a cost of 20 to the default route sent into area 10.15.0.0:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 201
RP/0/RP0/CPU0:router(config-ospfv3)# area 10.15.0.0
RP/0/RP0/CPU0:router(config-ospfv3-ar)# stub
RP/0/RP0/CPU0:router(config-ospfv3-ar)# default-cost 20
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface pos0/3/0/1
```

Related Commands

Command	Description
stub (OSPFv3)	Defines an area as a stub area.

R3.3 Beta Draft—Cisco Confidential Information**default-information originate (OSPFv3)**

To generate a default external route into an Open Shortest Path First Version 3 (OSPFv3) routing domain, use the **default-information originate** command in router ospfv3 configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [*policy policy-name*] [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**tag** *tag-value*]

no default-information originate [*policy policy-name*] [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**tag** *tag-value*]

Syntax Description

policy <i>policy-name</i>	(Optional) Specifies the policy to apply to default information origination.
always	(Optional) Always advertises the default route regardless of whether the software has a default route.
metric <i>metric-value</i>	(Optional) Specifies a metric used for generating the default route. If you omit a value and do not specify a value using the default-metric command, the default metric value is 10. The value used is specific to the protocol.
metric-type <i>type-value</i>	(Optional) Specifies an external link type associated with the default route advertised into the OSPFv3 routing domain. It can be one of the following values: 1—Type 1 external route 2—Type 2 external route
tag <i>tag-value</i>	(Optional) 32-bit dotted-decimal value attached to each external route. This is not used by the OSPFv3 protocol itself. It may be used to communicate information between Autonomous System Boundary Routers (ASBRs). If a tag is not specified, then zero (0) is used.

Defaults

A default external route into an OSPFv3 routing domain is not generated.

metric-value: 10

type-value: Type 2

Command Modes

Router ospfv3 configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The policy policy-name keyword and argument were added.
Release 3.3	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Whenever you use the **redistribute** or **default-information** command to redistribute routes into an OSPFv3 routing domain, the software automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the OSPFv3 routing domain. The software still must have a default route for itself before it generates one, except when you have specified the **always** keyword.

When you use the **default-information originate** command for the OSPFv3 process, the default network must reside in the routing table.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to specify a metric of 100 for the default route redistributed into the OSPFv3 routing domain and an external metric type of Type 1:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 109  
RP/0/RP0/CPU0:router(config-ospfv3)# default-information originate metric 100 metric-type 1
```

Related Commands

Command	Description
redistribute (OSPFv3)	Redistributes routes from one routing domain into another routing domain.

R3.3 Beta Draft—Cisco Confidential Information

default-metric (OSPFv3)

To set default metric values for routes redistributed from another protocol into Open Shortest Path First Version 3 (OSPFv3), use the **default-metric** command in router ospfv3 configuration mode. To return to the default state, use the **no** form of this command.

default-metric *value*

no default-metric *value*

Syntax Description	<i>value</i>	Default metric value appropriate for the specified routing protocol.

Defaults	Built-in, automatic metric translations, as appropriate for each routing protocol

Command Modes	Router ospfv3 configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the default-metric command with the redistribute command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, use a default metric to provide a reasonable substitute and enable the redistribution to proceed.

Task ID	Task ID	Operations
	ospf	read, write

Examples	The following example shows how to configure a router with both the Intermediate System-to-Intermediate System (IS-IS) and the OSPFv3 routing protocols. The OSPFv3 routing protocol advertises IS-IS derived routes and assigns the routes a metric of 10:
	RP/0/RP0/CPU0:router(config)# router ospfv3 1
	RP/0/RP0/CPU0:router(config-ospfv3)# default-metric 10
	RP/0/RP0/CPU0:router(config-ospfv3)# redistribute isis 109

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	redistribute (OSPFv3)	Redistributes routes from one routing domain into another routing domain.

R3.3 Beta Draft—Cisco Confidential Information**demand-circuit (OSPFv3)**

To configure the Open Shortest Path First Version 3 (OSPFv3) router process to treat the interface as an OSPFv3 demand circuit, use the **demand-circuit** command in the appropriate configuration mode. To remove the demand circuit designation from the interface, use the **no** form of this command.

demand-circuit [**disable**]

no demand-circuit

Syntax Description

disable	(Optional) Disables the demand circuit configuration that may have been specified at a higher level in the configuration.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the demand circuit parameter specified for the area.

If this command is not specified in area configuration mode, then the interface adopts the demand circuit parameter specified for the process.

If this command is not specified at any level, then the interface is not a demand circuit.

Command Modes

Interface configuration
Area configuration
Router ospfv3 configuration
Virtual-link configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

On point-to-point interfaces, only one end of the demand circuit must be configured with the **demand-circuit** command. Periodic hello messages are suppressed and periodic refreshes of link-state advertisements (LSAs) do not flood the demand circuit. This command allows the underlying data link layer to be closed when the topology is stable. In point-to-multipoint topology, only the multipoint end must be configured with this command.

Task ID

Task ID	Operations
ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to configure Packet-over-SONET (POS) interface 0/3/0/1 as an on-demand circuit:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1  
RP/0/RP0/CPU0:router(config-ospfv3)# area 0  
RP/0/RP0/CPU0:router(config-ospfv3)# interface POS 0/3/0/1  
RP/0/RP0/CPU0:router(config-ospfv3-if)# demand-circuit
```

R3.3 Beta Draft—Cisco Confidential Information

distance ospfv3

To define the Open Shortest Path First Version 3 (OSPFv3) route administrative distances based on route type, use the **distance ospfv3** command in router ospfv3 configuration mode. To restore the default value, use the **no** form of this command.

distance ospfv3 {intra-area | inter-area | external} *distance*

no distance ospfv3

Syntax Description	intra-area inter-area external	Type of area. It can be one of the following values: intra-area—All routes within an area. inter-area—All routes from one area to another area. external—All routes from other routing domains, learned by redistribution.
	distance	The route administrative distance.

Defaults *distance*: 110

Command Modes Router ospfv3 configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You must specify one of the keywords.

Use the **distance ospfv3** command to perform the same function as the **distance** command used with an access list. However, the **distance ospfv3** command sets a distance for an entire group of routes, rather than a specific route that passes an access list.

A common reason to use the **distance ospfv3** command is when you have multiple OSPFv3 processes with mutual redistribution, and you want to prefer internal routes from one over external routes from the other.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows how to change the external distance to 200, making it less reliable:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# redistribute ospfv3 2
RP/0/RP0/CPU0:router(config-ospfv3)# distance ospfv3 external 200
RP/0/RP0/CPU0:router(config-ospfv3)# exit
RP/0/RP0/CPU0:router(config)# router ospfv3 2
RP/0/RP0/CPU0:router(config-ospfv3)# redistribute ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# distance ospfv3 external 200
```

Related Commands	Command	Description
	distance (IP)	Defines an administrative distance.

R3.3 Beta Draft—Cisco Confidential Information

distribute-list prefix-list in

To filter the routes that Open Shortest Path First Version 3 (OSPFv3) installs in the Routing Information Base (RIB), use the **distribute-list prefix-list in** command in the appropriate configuration mode. To remove the filter, use the **no** form of this command.

distribute-list prefix-list *prefix-list-name* **in**

no distribute-list prefix-list *prefix-list-name* **in**

Syntax Description

<i>prefix-list-name</i>	IP Version 6 (IPv6) prefix list name. The list defines which IPv6 prefixes are installed in the RIB.

Defaults

All routes learned by OSPFv3 are installed in the RIB.

Command Modes

Interface configuration
Router ospfv3 configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **distribute-list prefix-list** command to limit the routes that OSPFv3 installs in the RIB of your router. This command does not affect the information sent to other OSPFv3 routers or the routes that these routers compute and install.

**Note**

Because the other OSPFv3 routers are not aware of any omissions in the RIB, they may send traffic addressed to the missing prefixes. If no other provision has been made for these prefixes, the packets are dropped.

When this command is specified in router ospfv3 configuration mode, the filter applies to all routes computed by OSPFv3.

When this command is specified in interface configuration mode, the filter applies only to routes that forward outgoing traffic over that interface.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows how to prevent OSPFv3 from installing any routes that have 2001:e624 as the first 32 bits of the address. OSPFv3 is also prevented from installing routes to 2002::/16 that use Packet-over-SONET (POS) interface 0/2/0/0 as the next-hop interface:

```
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list preflist1
RP/0/RP0/CPU0:router(config-ipv6-pfx)# deny 2001:e624::/32 le 128
RP/0/RP0/CPU0:router(config-ipv6-pfx)# permit ::/0 le 128
!
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list preflist2
RP/0/RP0/CPU0:router(config-ipv6-pfx)# deny 2002::/16
RP/0/RP0/CPU0:router(config-ipv6-pfx)# permit ::/0 le 128
!
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# distribute-list prefix-list preflist1 in
RP/0/RP0/CPU0:router(config-ospfv3)# area 1
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/2/0/0
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# distribute-list prefix-list preflist2 in
!
```

R3.3 Beta Draft—Cisco Confidential Information

distribute-list prefix-list out

To filter the routes redistributed into Open Shortest Path First Version 3 (OSPFv3) from other routing protocols, use the **distribute-list prefix-list out** command in router ospfv3 configuration mode. To remove the filter, use the **no** form of this command.

distribute-list prefix-list *prefix-list-name* **out** [*protocol* [*process-id*]]

no distribute-list prefix-list *prefix-list-name* **out** [*protocol* [*process-id*]]

Syntax Description

<i>prefix-list-name</i>	IP Version 6 (IPv6) prefix list name. The list defines which IPv6 prefixes are installed in the RIB.
<i>protocol</i>	(Optional) Source protocol from which routes are being redistributed. It can be one of the following keywords: bgp , isis , ospfv3 , static , and connected . The static keyword is used to redistribute IPv6 static routes. The connected keyword refers to routes that are established automatically because IPv6 is enabled on an interface. For routing protocols such as OSPFv3 and Intermediate System-to-Intermediate System (IS-IS), these routes are redistributed as external to the autonomous system.
<i>process-id</i>	(Optional) For the bgp keyword, an autonomous system number, which is a 16-bit decimal number. For the isis keyword, an optional argument that defines a meaningful name for a routing process. You can specify only one IS-IS process for each router. Creating a name for a routing process means that you use names when configuring routing. For the ospfv3 keyword, an appropriate OSPFv3 process name from which routes are to be redistributed. The value takes the form of a string. A decimal number can be entered, but it is stored internally as a string.

Defaults

All routes from protocols specified in the **redistribute (OSPFv3)** command are redistributed into OSPFv3.

Command Modes

Router ospfv3 configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Routes may be redistributed into OSPFv3 from several other routing protocols or from other OSPFv3 processes. These routes are then communicated to other OSPFv3 routes through Type 5 (External) or Type 7 not-so-stubby area (NSSA) link-state advertisements (LSAs). Use the **distribute-list prefix-list out** command to control redistribution by matching redistributed routes against an IPv6 prefix list. Only routes permitted by the prefix list are redistributed into OSPFv3.

Each protocol being redistributed into OSPFv3 may have a separate prefix list. In addition, a prefix list can be defined that applies to all protocols.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to prevent OSPFv3 from redistributing routes that have 2001:e624 as the first 32 bits of the address. In addition, routes with a prefix beginning with 2064 are not redistributed from Border Gateway Protocol (BGP) autonomous system 1, and only those routes are redistributed from BGP autonomous system 5.

```
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list p1
RP/0/RP0/CPU0:router(config-ipv6-pfx)# deny 2001:e624::/32 le 128
RP/0/RP0/CPU0:router(config-ipv6-pfx)# permit ::/0 le 128
!
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list p2
RP/0/RP0/CPU0:router(config-ipv6-pfx)# deny 2064::/16 le 128
RP/0/RP0/CPU0:router(config-ipv6-pfx)# permit ::/0 le 128
!
RP/0/RP0/CPU0:router(config)# ipv6 prefix-list p3
RP/0/RP0/CPU0:router(config-ipv6-pfx)# permit 2064::/16 le 128
!
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# redistribute bgp 1
RP/0/RP0/CPU0:router(config-ospfv3)# redistribute bgp 5
RP/0/RP0/CPU0:router(config-ospfv3)# distribute-list prefix-list p1 out
RP/0/RP0/CPU0:router(config-ospfv3)# distribute-list prefix-list p2 out bgp 1
RP/0/RP0/CPU0:router(config-ospfv3)# distribute-list prefix-list p3 out bgp 5
!
!
```

Related Commands

Command	Description
redistribute (OSPFv3)	Redistributes routes from one routing domain into another routing domain for OSPFv3.

R3.3 Beta Draft—Cisco Confidential Information**flood-reduction (OSPFv3)**

To suppress the unnecessary flooding of link-state advertisements (LSAs) in stable topologies, use the **flood-reduction** command in the appropriate configuration mode. To disable this feature, use the **no** form of this command.

flood-reduction [**disable** | **enable**]

no flood-reduction

Syntax Description	disable	(Optional) Disables the flood reduction configuration that may have been specified at a higher level in the configuration.
	enable	(Optional) Enables the flood reduction configuration that may have been specified at a higher level in the configuration.

Defaults	If this command is not specified in interface configuration mode, then the interface adopts the flood reduction parameter specified by area.
	If this command is not specified in area configuration mode, then the interface adopts the flood reduction parameter specified for the process.
	If this command is not specified at any level, then flood reduction is disabled.

Command Modes	Interface configuration
	Area configuration
	Router ospfv3 configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	All routers that support Open Shortest Path First Version 3 (OSPFv3) demand circuits are compatible with routers supporting flooding reduction.

Task ID	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to reduce the flooding of unnecessary LSAs for area 0:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1  
RP/0/RP0/CPU0:router(config-ospfv3)# area 0  
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/1/0/3  
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# flood-reduction
```

Related Commands

Command	Description
show ospfv3 interface	Displays OSPFv3-related interface information.
show ospfv3 neighbor	Displays OSPFv3 neighbor information on an individual interface basis.

R3.3 Beta Draft—Cisco Confidential Information

graceful-restart (OSPFv3)

To enable Graceful Restart, use the **graceful-restart** command in router ospfv3 configuration mode. To disable this feature, use the **no** form of this command.

graceful-restart [**helper disable** | **interval** *interval* | **lifetime** *lifetime*]

no graceful-restart [**helper disable** | **interval** *interval* | **lifetime** *lifetime*]

Syntax Description	helper disable	(Optional) Disables the routers helper support level.
	interval <i>interval</i>	(Optional) Specifies the minimum interval between Graceful Restarts. Range is 90 to 3600 seconds.
	lifetime <i>lifetime</i>	(Optional) Specifies the maximum route lifetime following a restart. Range is 90 to 3600 seconds.

Defaults This command has no defaults.

Command Modes Router ospfv3 configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	ospf	read, write

Examples The following example shows how to enable the Graceful Restart feature with a minimum interval between restarts of 300 seconds:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# graceful-restart interval 300
```


R3.3 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	show ospfv3 interface	Displays OSPFv3-related interface information.
	show ospfv3 neighbor	Displays OSPFv3 neighbor information on an individual interface basis.

R3.3 Beta Draft—Cisco Confidential Information

hello-interval (OSPFv3)

To specify the interval between hello packets that Open Shortest Path First Version 3 (OSPFv3) sends on an interface, use the **hello-interval** command in the appropriate configuration mode. To return to the default time, use the **no** form of this command.

hello-interval *seconds*

no hello-interval

Syntax Description

<i>seconds</i>	Interval (in seconds). The value must be the same for all nodes on a specific network.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the hello interval parameter specified by area.

If this command is not specified in area configuration mode, then the interface adopts the hello interval parameter specified for the process.

If this command is not specified at any level, then the hello interval is 10 seconds (broadcast) or 30 seconds (nonbroadcast).

Command Modes

Interface configuration
Area configuration
Router ospfv3 configuration
Virtual-link configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The hello interval value is advertised in the hello packets. The shorter the hello interval, the faster topological changes are detected, but more routing traffic ensues. This value must be the same for all routers and access servers on a specific network.

Task ID

Task ID	Operations
ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to set the interval between hello packets to 15 seconds on Packet-over-SONET (POS) interface 0/3/0/2:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# area 0
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/3/0/2
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# hello-interval 15
```

Related Commands

Command	Description
dead-interval (OSPFv3)	Sets the interval after which a neighbor is declared dead when no hello packets are observed

R3.3 Beta Draft—Cisco Confidential Information

instance

To set the 8-bit instance ID used in Open Shortest Path First Version 3 (OSPFv3) packets sent on an interface, use the **instance** command in the appropriate configuration mode. To remove the instance ID, use the **no** form of this command.

instance *instance-id*

no instance *instance-id*

Syntax Description

<i>instance-id</i>	Instance identifier sent in OSPFv3 packets. Range is 0 to 255. The same value must be used by all the communicating OSPFv3 routers on a link.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the instance parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the instance parameter specified for the process.

If this command is not specified at any level, then the instance is 0.

Command Modes

Interface configuration
Area configuration
Router ospfv3 configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The OSPFv3 routing protocol allows multiple unrelated OSPFv3 processes to share a link by using an 8-bit “instance” value to demultiplex the protocol packets. Each OSPFv3 process sets its configured instance value in the OSPFv3 packets that it sends, and ignores received packets with instance values from other OSPFv3 processes.

**Note**

The *instance-id* argument should not be confused with the *process-name* argument that is specified by the **router ospfv3** command. The former is an 8-bit integer that is sent to other routers as part of the OSPFv3 protocol, and the latter is a 1- to 40-character ASCII string that is significant only within a given

R3.3 Beta Draft—Cisco Confidential Information

router. The instance ID value is also unrelated to the router ID that is specified by the **router-id** command, which is a 32-bit integer value that uniquely identifies a router within an OSPFv3 routing domain.

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows how to set the instance value for Packet-over-SONET (POS) interface 0/3/0/1 to 42:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# area 0
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# instance 42
```

Related Commands	Command	Description
	router ospfv3	Configures an OSPFv3 routing process.
	router-id (OSPFv3)	Configures a router ID for the OSPFv3 routing process

R3.3 Beta Draft—Cisco Confidential Information

interface (OSPFv3)

To define the interfaces on which Open Shortest Path First Version 3 (OSPFv3) runs, use the **interface** command in area configuration mode. To disable OSPFv3 routing for an interface, use the **no** form of this command.

interface *type instance*

no interface *type instance*

Syntax Description

<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a Route Processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults

An interface is not defined.

Command Modes

Area configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **interface** command to associate a specific interface with an OSPFv3 area. The interface remains associated with the area even when the IPv6 address of the interface changes.

This command places the router in interface configuration mode (prompt: config-router-ar-if), from which you can configure interface-specific settings. Commands configured under this mode (such as the **cost** command) are automatically bound to that interface.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to define two interfaces that belong to area 1. The cost value for packets on Packet-over-SONET (POS) interface 0/3/0/1 is set at 40; the cost value for POS interface 0/3/0/2 is 65:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# area 1
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# cost 40
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# exit
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/3/0/2
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# cost 65
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# exit
```

R3.3 Beta Draft—Cisco Confidential Information

log adjacency changes (OSPFv3)

To change the default syslog messages for Open Shortest Path First Version 3 (OSPFv3) neighbor state changes, use the **log adjacency changes** command in router configuration mode. To suppress all adjacency change messages, use the **disable** keyword.

log adjacency changes [**detail**] [**disable**]

Syntax Description	detail	(Optional) Provides detailed information about adjacency changes.
	disable	(Optional) Disables the neighbor state change messages.

Defaults Neighbor state change messages are enabled.

Command Modes Router ospfv3 configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

By default, you are notified of OSPFv3 neighbor changes without explicitly configuring the **log adjacency changes** command. The syslog messages that are sent provide a high-level view of changes to the state of the OSPFv3 peer relationship.

Task ID	Task ID	Operations
	ospf	read, write

Examples The following example shows how to disable neighbor state change messages:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# log adjacency changes disable
```

The following example shows how to re-enable syslog messages for any OSPFv3 neighbor state changes:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# log adjacency changes
```


R3.3 Beta Draft—Cisco Confidential Information

maximum interfaces (OSPFv3)

To control the maximum number of interfaces that can be configured under an Open Shortest Path First Version 3 (OSPFv3) process, use the **maximum interfaces** command in the router ospfv3 configuration mode. To remove the **maximum interfaces** command from the configuration file and restore the system to its default condition with respect to the routing protocol, use the **no** form of this command.

maximum interfaces *value*

no maximum interfaces

Syntax Description	<i>value</i>	Maximum number of interfaces that can be configured for this OSPFv3 process. Range is 1 to 1024.

Defaults	<i>value</i> : 255 interfaces

Command Modes	Router ospfv3 configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	ospf	read, write

Examples	The following example shows how to allow a maximum of 500 interfaces in an OSPFv3 process:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# maximum interfaces 500
```

R3.3 Beta Draft—Cisco Confidential Information

maximum paths (OSPFv3)

To control the maximum number of parallel routes that the Open Shortest Path First Version 3 (OSPFv3) can support, use the **maximum paths** command in router ospfv3 configuration mode. To remove the **maximum paths** command from the configuration file and restore the system to its default condition with respect to the routing protocol, use the **no** form of this command.

maximum paths *routes-number*

no maximum paths

Syntax Description	<i>routes-number</i>	Maximum number of parallel routes that OSPFv3 can install in a routing table. Range is 1 to 32 for Cisco CRS-1s and 1 to 16 for Cisco XR 12000 Series Routers.

Defaults	Cisco CRS-1s: 16 paths Cisco XR 12000 Series Routers: 16 paths

Command Modes	Router ospfv3 configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	ospf	read, write

Examples	The following example shows how to allow a maximum of two paths to a destination:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# maximum paths 2
```

R3.3 Beta Draft—Cisco Confidential Information

maximum redistributed-prefixes (OSPFv3)

To limit the number of prefixes redistributed into Open Shortest Path First Version 3 (OSPFv3) or to generate a warning when the number of prefixes redistributed into OSPFv3 reaches a maximum, use the **maximum redistributed-prefixes** command in router configuration mode. To remove the values, use the **no** form of this command.

maximum redistributed-prefixes *limit* [*threshold*] [**warning-only**]

no maximum redistributed-prefixes

Syntax Description		
<i>limit</i>		Maximum number of IP Version 6 (IPv6) prefixes that are allowed to be redistributed into OSPFv3, or, if the warning-only keyword is present, sets the number of prefixes allowed to be redistributed into OSPFv3 before the system logs a warning message. Range is 1 to 4294967295.
		Note If the warning-only keyword is also configured, this value does not limit redistribution; it is simply the number of redistributed prefixes that, when reached, causes a warning message to be logged.
<i>threshold</i>		(Optional) Percentage of the value set for the maximum number of redistributed prefixes that, when reached, causes a warning message to be logged.
warning-only		(Optional) Causes a warning to be logged when the number of routes defined by the <i>limit</i> argument have been redistributed. Additional redistribution is not prevented.

Defaults

limit: 10240
threshold: 75 percent

Command Modes Router ospfv3 configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If someone mistakenly injects a large number of IPv6 routes into OSPFv3, perhaps by redistributing Border Gateway Protocol (BGP) into OSPFv3, the network can be severely flooded. Limiting the number of redistributed routes prevents this potential problem.

R3.3 Beta Draft – Cisco Confidential Information

When the **maximum redistributed-prefixes** command is configured, if the number of redistributed routes reaches the maximum value configured, no more routes are redistributed (unless the **warning-only** keyword is configured).

The redistribution limit applies only to external IPv6 prefixes. Default routes and summarized routes are not limited.

The limit is tracked separately for each not-so-stubby-area (NSSA) because redistribution to NSSAs is done independently for each NSSA and independently of all other regular areas.

Select a maximum value based on your knowledge of how many prefixes are redistributed on the router to the OSPFv3 process.

Task ID	Task ID	Operations
	ospf	read, write

Examples

This example shows how to set a maximum of 2000 prefixes that can be redistributed into OSPFv3 process 1. If the number of prefixes redistributed reaches 75 percent of 2000 (1500 prefixes), a warning message is logged. Another warning is logged if the limit is reached and no more routes are redistributed.

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# redistribute bgp 2406
RP/0/RP0/CPU0:router(config-ospfv3)# maximum redistributed-prefixes 2000
```

R3.3 Beta Draft—Cisco Confidential Information

mtu-ignore (OSPFv3)

To prevent the Open Shortest Path First Version 3 (OSPFv3) router process from checking whether neighbors are using the same maximum transmission unit (MTU) on a common interface when exchanging database descriptor (DBD) packets, use the **mtu-ignore** command in the appropriate configuration mode. To return to the default state, use the **no** form of this command.

mtu-ignore [**disable** | **enable**]

no mtu-ignore

Syntax Description	disable	(Optional) Disables the attribute in instances in which it is specified at a higher level in the configuration. Note The disable keyword is not available in router ospfv3 configuration mode.
	enable	(Optional) Enables the attribute in instances where it is specified at a higher level in the configuration.

Defaults	If this command is not specified in interface configuration mode, then the interface adopts the MTU ignore parameter specified by the area. If this command is not specified in area configuration mode, then the interface adopts the MTU ignore parameter specified for the process. If this command is not specified at any level, then OSPFv3 checks the MTU received from neighbors when exchanging DBD packets.

Command Modes	Interface configuration Area configuration Router ospfv3 configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the mtu-ignore command to check whether OSPFv3 neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DBD packets. If the receiving MTU in the DBD packet is higher than the MTU configured on the incoming interface, OSPF adjacency is not established.

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	ospf	read, write

Examples The following example shows how to disable MTU mismatch detection on received DBD packets on Packet-over-SONET (POS) interface 0/1/0/3:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# area 0
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/1/0/3
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# mtu-ignore
```

R3.3 Beta Draft—Cisco Confidential Information**neighbor (OSPFv3)**

To configure Open Shortest Path First Version 3 (OSPFv3) routers interconnecting to nonbroadcast networks, use the **neighbor** command in interface configuration mode. To remove a configuration, use the **no** form of this command.

neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter** **all out**]

no neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter** **all out**]

Syntax Description		
<i>ipv6-address</i>		Link-local IP Version 6 (IPv6) address of the neighbor. This argument must be in the form documented in RFC 2373, in which the address is specified in hexadecimal using 16-bit values between colons.
priority <i>number</i>		(Optional) Specifies an 8-bit number indicating the router priority value of the nonbroadcast neighbor associated with the IP address specified. The priority keyword does not apply to point-to-multipoint interfaces.
poll-interval <i>seconds</i>		(Optional) Specifies an unsigned integer value (in seconds) reflecting the poll interval. RFC 1247 recommends that this value be much larger than the hello interval. The poll-interval keyword does not apply to point-to-multipoint interfaces.
cost <i>number</i>		(Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured assume the cost of the interface, based on the cost command. On point-to-multipoint interfaces, cost <i>number</i> is the only keyword and argument combination that works. The cost keyword does not apply to nonbroadcast multiaccess (NBMA) networks.
database-filter all out		(Optional) Filters outgoing link-state advertisements (LSAs) to an OSPFv3 neighbor.

Defaults	No configuration is specified. priority <i>number</i> : 0 poll-interval <i>seconds</i> : 120 seconds (2 minutes)

Command Modes	Interface configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

One neighbor entry must be included in the software configuration for each known nonbroadcast network neighbor. The neighbor address must be the IPv6 link-local address of the interface.

If a neighboring router has become inactive (hello packets have not been seen for the router dead interval period), it may still be necessary to send hello packets to the dead neighbor. These hello packets are sent at a reduced rate called the poll interval.

When the router starts up, it sends only hello packets to those routers with nonzero priority; that is, routers that are eligible to become designated routers (DRs) and backup designated routers (BDRs). After the DR and BDR are selected, the DR and BDR then start sending hello packets to all neighbors to form adjacencies.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to declare a router at address fe80::3203:a0ff:fe9d:f3fe on a nonbroadcast network:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# area 0
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/2/0/0
RP/0/RP0/CPU0:router(config-ospfv3-ar)# network non-broadcast
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# neighbor fe80::3203:a0ff:fe9d:f3fe
```

Related Commands

Command	Description
priority (OSPFv3)	Sets the router priority, which helps determine the designated router for this network.

R3.3 Beta Draft—Cisco Confidential Information

network (OSPFv3)

To configure the Open Shortest Path First Version 3 (OSPFv3) network type to a type other than the default for a given medium, use the **network** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

network { **broadcast** | **non-broadcast** | { **point-to-multipoint** [**non-broadcast**] | **point-to-point** } }

no network

Syntax Description

broadcast	Sets the network type to broadcast.
non-broadcast	Sets the network type to nonbroadcast multiaccess (NBMA).
point-to-multipoint	Sets the network type to point-to-multipoint.
[non-broadcast]	(Optional) Sets the point-to-multipoint network to be nonbroadcast. If you use the non-broadcast keyword, the neighbor command is required.
point-to-point	Sets the network type to point-to-point.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the network parameter specified by the area.
 If this command is not specified in area configuration mode, then the interface adopts the network parameter specified for the process.
 If this command is not specified at any level, then the OSPFv3 network type is the default of the given medium.

Command Modes

Interface configuration
 Area configuration
 Router ospfv3 configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **network** command to configure broadcast networks as NBMA networks when, for example, routers in your network do not support multicast addressing.

R3.3 Beta Draft—Cisco Confidential Information

Configuring NBMA networks as either broadcast or nonbroadcast assumes that there are virtual circuits from every router to every router or fully meshed network. However, there are other configurations where this assumption is not true; for example, a partially meshed network. In these cases, you can configure the OSPFv3 network type as a point-to-multipoint network. Routing between two routers that are not directly connected goes through the router that has virtual circuits to both routers. You need not configure neighbors when using this command.

If the **network** command is issued on an interface that does not allow it, this command is ignored.

OSPFv3 has two features related to point-to-multipoint networks. One feature applies to broadcast networks and the other feature applies to nonbroadcast networks:

- On point-to-multipoint, broadcast networks, you can use the **neighbor** command, and you must specify a cost to that neighbor.
- On point-to-multipoint, nonbroadcast networks, you must use the **neighbor** command to identify neighbors. Assigning a cost to a neighbor is optional.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure an Ethernet interface as point-to-point:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# area 0
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface TenGigE0/1/0/3
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# network point-to-point
```

Related Commands

Command	Description
neighbor (OSPFv3)	Configures OSPFv3 routers interconnecting to nonbroadcast networks.

R3.3 Beta Draft—Cisco Confidential Information**nssa (OSPFv3)**

To configure an area as a not-so-stubby area (NSSA), use the **nssa** command in area configuration mode. To remove the NSSA distinction from the area, use the **no** form of this command.

nssa [**no-redistribution**] [**default-information-originate** [**metric** *metric-value* | **metric-type** *type-value*]] [**no-summary**]

no nssa

Syntax Description

no-redistribution	(Optional) Imports routes only into the normal areas, but not into the NSSA area, by the redistribute command when the router is an NSSA Area Border Router (ABR).
default-information-originate	(Optional) Generates a Type 7 default into the NSSA area. This keyword takes effect only on an NSSA ABR or NSSA Autonomous System Boundary Router (ASBR).
metric <i>metric-value</i>	(Optional) Specifies a metric used for generating the default route. If you omit a value and do not specify a value using the default-metric command, the default metric value is 10. The value used is specific to the protocol.
metric-type <i>type-value</i>	(Optional) Specifies an external link type associated with the default route advertised into the Open Shortest Path First Version 3 (OSPFv3) routing domain. It can be one of the following values: 1—Type 1 external route 2—Type 2 external route
no-summary	(Optional) Prevents an (ABR) from sending summary link advertisements into the NSSA area.

Defaults

No NSSA area is defined.
If you do not specify a value using the **default-metric** command, the default metric value is 10.
The default *type-value* is Type 2 external route.

Command Modes

Area configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft – Cisco Confidential Information

A default route need not be defined in an NSSA ABR when the **nssa** command is configured. However, if this command is configured on an NSSA ASBR, then a default route must be defined.



Note

NSSA cannot be configured for area 0 (backbone area).

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure area 1 as an NSSA area:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# router-id 10.18.1.1
RP/0/RP0/CPU0:router(config-ospfv3)# area 1
RP/0/RP0/CPU0:router(config-ospfv3-ar)# nssa
```

R3.3 Beta Draft—Cisco Confidential Information

ospfv3 name-lookup

To configure Open Shortest Path First Version 3 (OSPFv3) to look up Domain Name System (DNS) names, use the **ospfv3 name-lookup** command in global configuration mode. To disable this function, use the **no** form of this command.

ospfv3 name-lookup

no ospfv3 name-lookup

Syntax Description

This command has no arguments or keywords.

Defaults

Routers are displayed by router ID or neighbor ID.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **ospfv3 name-lookup** command to simplify the task of searching for a router. Routers are displayed by name rather than by router ID or neighbor ID.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to configure OSPFv3 to look up DNS names for use in all OSPFv3 **show** command displays:

```
RP/0/RP0/CPU0:router(config)# ospfv3 name-lookup
```

R3.3 Beta Draft—Cisco Confidential Information

passive (OSPFv3)

To suppress the sending of Open Shortest Path First Version 3 (OSPFv3) packets on an interface, use the **passive** command in the appropriate configuration mode. To remove the passive configuration, use the **no** form of this command.

passive [**disable**]

no passive

Syntax Description

disable	(Optional) Sends OSPFv3 updates.
Note	The disable keyword is not available in router ospfv3 configuration mode.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the passive parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the passive parameter specified for the process.

If this command is not specified at any level, then the passive parameter is disabled and OSPFv3 updates are sent on the interface.

Command Modes

Interface configuration
Area configuration
Router ospfv3 configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

OSPF routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF domain.

Task ID

Task ID	Operations
ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows that OSPFv3 updates run over Packet-over-SONET (POS) interface 0/3/0/0, 0/2/0/0, and 0/2/0/2. All other interfaces suppress sending OSPFv3 updates because they are in passive mode.

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# router-id 10.0.0.206
RP/0/RP0/CPU0:router(config-ospfv3)# passive
RP/0/RP0/CPU0:router(config-ospfv3)# area 0
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/3/0/0
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# passive disable
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# exit
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/3/0/1
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# exit
RP/0/RP0/CPU0:router(config-ospfv3-ar)# exit
RP/0/RP0/CPU0:router(config-ospfv3)# area 1
RP/0/RP0/CPU0:router(config-ospfv3-ar)# passive disable
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/2/0/0
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# exit
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/2/0/1
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# passive
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# exit
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/2/0/2
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# exit
```

R3.3 Beta Draft—Cisco Confidential Information

priority (OSPFv3)

To set the router priority for an interface, which helps determine the designated router for an Open Shortest Path First Version 3 (OSPFv3) link, use the **priority** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

priority *value*

no priority

Syntax Description

<i>value</i>	8-bit unsigned integer indicating the router priority value. Range is 0 to 255.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the priority parameter specified by the area.

If this command is not specified in area configuration mode, then the interface adopts the priority parameter specified by the process.

If this command is not specified at any level, then the default priority is 1.

Command Modes

Interface configuration
Area configuration
Router ospfv3 configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to broadcast and nonbroadcast multiaccess (NBMA) networks.

Task ID

Task ID	Operations
ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to set the router priority value to 4 on Packet-over-SONET (POS) interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# area 0
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# priority 4
```

Related Commands

Command	Description
neighbor (OSPFv3)	Configures OSPFv3 routers interconnecting to nonbroadcast networks.
network (OSPFv3)	Configures the OSPFv3 network type to a type other than the default for a given medium.

R3.3 Beta Draft—Cisco Confidential Information

range (OSPFv3)

To consolidate and summarize routes at an area boundary for Open Shortest Path First Version 3 (OSPFv3), use the **range** command in area configuration mode. To restore the default values, use the **no** form of this command.

range *ipv6-prefix/prefix-length* [**advertise** | **not-advertise**] [**cost** *number*]

no range *ipv6-prefix/prefix-length* [**advertise** | **not-advertise**] [**cost** *number*]

Syntax Description	<i>ipv6-prefix</i>	Summary prefix designated for a range of IP Version 6 (IPv6) prefixes. This argument must be in the form documented in RFC 2373, in which the address is specified in hexadecimal using 16-bit values between colons.
	<i>/prefix-length</i>	Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value.
	advertise	(Optional) Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA).
	not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed and the component networks remain hidden from other networks.
	cost <i>number</i>	(Optional) Specifies a cost for the range. Range is 1 to 16777214.

Defaults Routes are not consolidated and summarized for an area.

Command Modes Area configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information

Use the **range** command only with Area Border Routers (ABRs). It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This process is called *route summarization*.

You can use the **range** command to configure multiple ranges. Thus, OSPFv3 can summarize addresses for many different sets of address ranges.

Task ID

Task ID	Operations

ospf	read, write

Examples

The following example shows how to specify one summary route to be advertised by the ABR to other areas for all IPv6 prefixes within the range defined by summary prefix 4004:f000::/32:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 201  
RP/0/RP0/CPU0:router(config-ospfv3)# area 0  
RP/0/RP0/CPU0:router(config-ospfv3-ar)# range 4004:f000::/32
```

R3.3 Beta Draft—Cisco Confidential Information

redistribute (OSPFv3)

To redistribute routes from one routing domain into Open Shortest Path First Version 3 (OSPFv3), use the **redistribute** command in router ospfv3 configuration mode. To remove the **redistribute** command from the configuration file and restore the system to its default condition in which the software does not redistribute routes, use the **no** form of this command.

Border Gateway Protocol (BGP)

redistribute bgp *process-id* [**metric** *metric-value*] [**metric-type** {1 | 2}] [**policy** *policy-name*] [**tag** *tag-value*]

no redistribute bgp *process-id* [**metric** *metric-value*] [**metric-type** {1 | 2}] [**policy** *policy-name*] [**tag** *tag-value*]

Local Interface Routes

redistribute connected [**metric** *metric-value*] [**metric-type** {1 | 2}] [**policy** *policy-name*] [**tag** *tag-value*]

no redistribute connected [**metric** *metric-value*] [**metric-type** {1 | 2}] [**policy** *policy-name*] [**tag** *tag-value*]

Intermediate System-to-Intermediate System (IS-IS)

redistribute isis *process-id* [**level-1** | **level-2** | **level-1-2**] [**metric** *metric-value*] [**metric-type** {1 | 2}] [**policy** *policy-name*] [**tag** *tag-value*]

no redistribute isis *process-id* [**level-1** | **level-2** | **level-1-2**] [**metric** *metric-value*] [**metric-type** {1 | 2}] [**policy** *policy-name*] [**tag** *tag-value*]

Open Shortest Path First Version 3 (OSPFv3)

redistribute ospfv3 *process-id* [**match** {**external** [1 | 2] | **internal** | **nssa-external** [1 | 2]]] [**metric** *metric-value*] [**metric-type** {1 | 2}] [**policy** *policy-name*] [**tag** *tag-value*]

no redistribute ospfv3 *process-id* [**match** {**external** [1 | 2] | **internal** | **nssa-external** [1 | 2]]] [**metric** *metric-value*] [**metric-type** {1 | 2}] [**policy** *policy-name*] [**tag** *tag-value*]

Static

redistribute static [**metric** *metric-value*] [**metric-type** {1 | 2}] [**policy** *policy-name*] [**tag** *tag-value*]

no redistribute static [**metric** *metric-value*] [**metric-type** {1 | 2}] [**policy** *policy-name*] [**tag** *tag-value*]

R3.3 Beta Draft—Cisco Confidential Information

Syntax Description		
bgp		Distributes routes from the BGP protocol.
<i>process-id</i>		For the bgp keyword, an autonomous system number, which is a 16-bit decimal number. Range is 1 to 65535. For the isis keyword, an IS-IS instance name from which routes are to be redistributed. The value takes the form of a string. A decimal number can be entered, but it is stored internally as a string. For the ospf keyword, an OSPF instance name from which routes are to be redistributed. The value takes the form of a string. A decimal number can be entered, but it is stored internally as a string.
metric <i>metric-value</i>		(Optional) Specifies the metric used for the redistributed route. Range is 1 to 16777214. Use a value consistent with the destination protocol.
metric-type {1 2}		(Optional) Specifies the external link type associated with the 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 no metric-type is specified, the default is Type 2 external routes.
tag <i>tag-value</i>		(Optional) Specifies the 32-bit dotted-decimal value attached to each external route. This value is not used by the OSPF protocol itself, but is carried in the External LSAs. Range is 0 to 4294967295.
policy <i>policy-name</i>		(Optional) Specifies the identifier of a configured policy. A policy is used to filter the importation of routes from this source routing protocol to OSPF.
connected		Distributes routes that are established automatically by virtue of having enabled IP on an interface.
isis		Distributes routes from the IS-IS protocol.
level-1		(Optional) Redistributes Level 1 routes into other IP routing protocols independently.
level-1-2		(Optional) Redistributes both Level 1 and Level 2 routes into other IP routing protocols.
level-2		(Optional) Redistributes Level 2 routes into other IP routing protocols independently.
ospf		Distributes routes from the OSPF protocol.

R3.3 Beta Draft—Cisco Confidential Information

match { internal external [1 2] nssa-external [1 2]}	(Optional) Specifies the criteria by which OSPF routes are redistributed into other routing domains. It can be one or more of the following: • internal—Routes that are internal to a specific autonomous system (intra- and inter-area OSPF routes). • external [1 2]—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 external routes. • nssa-external [1 2]—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 not-so-stubby area (NSSA) external routes. For the external and nssa-external options, if a type is not specified, then both Type 1 and Type 2 are assumed. If no match is specified, the default is no filtering.
static	Redistributes IP static routes.

Defaults

Route redistribution is disabled.

metric *metric-value*: Default is 20 for routes from all protocols except BGP routes, in which the default is 1.

metric-type *type-value*: Type 2 external route

All routes from the OSPFv3 routing protocol are redistributed.

tag *tag-value*: If no value is specified, the remote autonomous system number is used for routes from Border Gateway Protocol (BGP); for other protocols, the default is 0.

Command Modes

Router ospfv3 configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Disabling or changing the arguments of any keyword does not affect the state of other keywords.

In general, route redistribution from Level 1 to Level 2 is automatic. You might want to use this command to better control which Level 1 routes can be redistributed into Level 2.

Level 2 routes redistributed into Level 1 is called *route leaking*. Route leaking is disabled by default. That is, Level 2 routes are not automatically included in Level 1 link-state protocols. If you want to leak Level 2 routes into Level 1, you must enable that behavior by using this command.

R3.3 Beta Draft—Cisco Confidential Information

Redistribution from Level 1 into Level 1 and from Level 2 into Level 2 is not allowed.

A router receiving a link-state packet with an internal metric considers the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric considers only the advertised metric to reach the destination.

Redistributed routing information should always be filtered by the **distribute-list prefix-list out** command. Use of this command ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

OSPFv3 Considerations

Whenever you use the **redistribute** or the **default-information** command to redistribute routes into an OSPFv3 routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a default route into the OSPFv3 routing domain.

When routes are redistributed between OSPFv3 processes, no OSPFv3 metrics are preserved.

When routes are redistributed into OSPF and no metric is specified with the **metric** keyword, OSPF uses 20 as the default metric for routes from all protocols except BGP routes, which get a metric of 1. Furthermore, when the router redistributes from one OSPFv3 process to another OSPFv3 process on the same router, and if no default metric is specified, the metrics in one process are carried to the redistributing process.

BGP Considerations

The only connected routes affected by this command are the routes not specified by the **network** (BGP) command.

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows how to cause static routes to be redistributed into an OSPFv3 domain:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 109
RP/0/RP0/CPU0:router(config-ospfv3)# redistribute isis level-1
```

Related Commands	Command	Description
	default-information originate (OSPFv3)	Redistributes routes into a routing domain.
	distribute-list prefix-list out	Filters the routes redistributed into OSPFv3 from other routing protocols.

R3.3 Beta Draft—Cisco Confidential Information**retransmit-interval (OSPFv3)**

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the Open Shortest Path First Version 3 (OSPFv3) interface, use the **retransmit-interval** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

retransmit-interval *seconds*

no retransmit-interval

Syntax Description

<i>seconds</i>	Time (in seconds) between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network. Range is 1 to 65535 seconds.

Defaults

If this command is not specified in interface configuration mode, then the interface adopts the retransmit interval parameter specified by the area.
 If this command is not specified in area configuration mode, then the interface adopts the retransmit interval parameter specified by the process.
 If this command is not specified at any level, then the default retransmit interval is 5 seconds.

Command Modes

Interface configuration
 Area configuration
 Router ospfv3 configuration
 Virtual-link configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When a router sends an LSA to its neighbor, it keeps the LSA until it receives the acknowledgment message. If the router receives no acknowledgment, it resends the LSA.

The setting of this parameter should be conservative, or needless retransmission results. The value should be larger for serial lines and virtual links.

Task ID

Task ID	Operations
ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to set the retransmit interval value to 8 seconds while in interface configuration mode:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1  
RP/0/RP0/CPU0:router(config-ospfv3)# area 0  
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/2/0/0  
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# retransmit-interval 8
```

R3.3 Beta Draft—Cisco Confidential Information**router-id (OSPFv3)**

To configure a router ID for the Open Shortest Path First Version 3 (OSPFv3) routing process, use the **router-id** command in router ospfv3 configuration mode. To cause the software to use the default method of determining the router ID, use the **no** form of this command.

router-id {*router-id* | *interface-type interface-instance*}

no router-id {*router-id* | *interface-type interface-instance*}

Syntax Description	
<i>router-id</i>	32-bit router ID value specified in four-part, dotted-decimal notation.
<i>interface-type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a Route Processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults If this command is not configured, the router ID is the highest IP address for an interface on the router, with any loopback interface taking precedence.

Command Modes Router ospfv3 configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

We recommend that you use the **router-id** command to explicitly specify a unique 32-bit numeric value for the router ID. This configuration ensures that OSPFv3 can function regardless of the interface address configuration.

OSPFv3 attempts to obtain a router ID from the following sources in the order of decreasing preference:

- The primary IPv4 address of the interface specified by the **router-id** (OSPFv3) command in router ospfv3 configuration mode.
- The 32-bit value configured by the **router-id** command in configuration mode. This value must be an IPv4 address assigned to an interface on your router.
- The primary IPv4 address of the interface configured by the **router-id** command in global configuration mode.
- The highest IPv4 address assigned to any loopback interface.

If the OSPFv3 process cannot obtain a router ID from any of these sources, the router issues the following error message:

```
%OSPFv3-4-NORTRID : OSPFv3 process 1 cannot run - configure a router ID for this process
```

At this point, OSPFv3 is effectively passive on all its interfaces. To run OSPFv3, make a router ID available by one of the methods described.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to assign the IP address of 10.0.0.10 to the OSPFv3 process 109:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 109
RP/0/RP0/CPU0:router(config-ospfv3)# router-id 10.0.0.10
```

Related Commands

Command	Description
clear ospfv3 process	Resets an OSPFv3 router process without stopping and restarting it.

R3.3 Beta Draft—Cisco Confidential Information

router ospfv3

To configure an Open Shortest Path First Version 3 (OSPFv3) routing process, use the **router ospfv3** command in global configuration mode. To terminate an OSPFv3 routing process, use the **no** form of this command.

router ospfv3 *process-name*

no router ospfv3 *process-name*

Syntax Description

<i>process-name</i>	Name that uniquely identifies an OSPFv3 routing process. The process name is any alphanumeric string no longer than 40 characters.

Defaults

No OSPFv3 routing process is defined.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You can specify multiple OSPFv3 routing processes in each router.

Task ID

Task ID	Operations
ospf	read, write

Examples

The following example shows how to instantiate an OSPFv3 routing process with a process name of 1:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
```

R3.3 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	area (OSPFv3)	Defines an OSPFv3 area.
	interface (OSPFv3)	Defines an OSPFv3 interface by type.

R3.3 Beta Draft—Cisco Confidential Information

show ospfv3

To display general information about Open Shortest Path First Version 3 (OSPFv3) routing processes, use the **show ospfv3** command in EXEC mode.

show ospfv3 [*process-name*]

Syntax Description

<i>process-name</i>	(Optional) Name that uniquely identifies an OSPFv3 routing process. The process name is defined by the router ospfv3 command. If this argument is included, only information for the specified routing process is displayed.

Defaults

No default behavior or value

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
ospf	read

Examples

The following sample output from the **show ospfv3** command:

```
RP/0/RP0/CPU0:router# show ospfv3 1
```

```
Routing Process "ospfv3 test" with ID 3.3.3.3
It is an autonomous system boundary router
Redistributing External Routes from,
static
Maximum number of redistributed prefixes 10240
Threshold for warning message 75%
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF 10000 msec
Maximum wait time between two consecutive SPF 10000 msec
Initial LSA throttle delay 0 msec
```

R3.3 Beta Draft—Cisco Confidential Information

```

Minimum hold time for LSA throttle 5000 msec
Maximum wait time for LSA throttle 5000 msec
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 sec
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Maximum number of configured interfaces 255
Number of external LSA 1. Checksum Sum 0x004468
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Area BACKBONE(0) (Inactive)
  Number of interfaces in this area is 1
  SPF algorithm executed 1 times
  Number of LSA 3. Checksum Sum 0x018109
  Number of DCbitless LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0

```

Table 96 describes the significant fields shown in the display.

Table 96 *show ospfv3 Field Descriptions*

Field	Description
Routing Process “ospfv3 test” with ID 3.3.3.3	OSPFv3 process name.
It is	Types are internal, area border, or autonomous system boundary.
Redistributing External Routes from	Lists of redistributed routes, by protocol.
Maximum number of redistributed prefixes	Number of redistributed prefixes
Threshold for warning message	Warning message threshold.
Initial SPF schedule delay	Delay time of SPF calculations.
Minimum hold time between two consecutive SPF	Minimum hold time between consecutive SPF.
Maximum wait time between two consecutive SPF	Maximum wait time between consecutive SPF.
Initial LSA throttle delay	LSA throttle delay.
Maximum hold time for LSA throttle	After initial throttle delay, the LSA generation is backed off by hold interval.
Maximum wait time for LSA throttle	Maximum throttle delay for LSA generation.
Minimum LSA arrival	Minimum LSA arrival.
LSA group pacing timer	Configured LSA group pacing timer (in seconds).
Interface flood pacing timer	Flooding pacing interval.
Retransmission pacing timer	Retransmission pacing interval.
Maximum number of configured interfaces	Maximum number of configured interfaces.
Number of external LSA	Number of external LSAs.
Number of areas in this router is	Number of areas configured for the router.

R3.3 Beta Draft—Cisco Confidential Information

Table 96 *show ospfv3 Field Descriptions (continued)*

Field	Description
Number of interfaces in this area is	Number of interfaces in the area.
SPF algorithm executed n times	Times SPF algorithm was executed.
Number of LSA	Number of LSAs.
Number of DCbitless LSA	Number of DCbitless LSAs.
Number of indication LSA	Number of indication LSAs.
Number of DoNotAge LSA	Number of do-not-age LSAs.
Flood list length	Flood list length.

Related Commands

Command	Description
router ospfv3	Configures an OSPFv3 routing process.

R3.3 Beta Draft—Cisco Confidential Information

show ospfv3 border-routers

To display the internal Open Shortest Path First Version 3 (OSPFv3) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the **show ospfv3 border-routers** command in EXEC mode.

show ospfv3 [*process-name*] **border-routers** [*router-id*]

Syntax Description	<i>process-name</i>	(Optional) Name that uniquely identifies an OSPFv3 routing process. The process name is defined by the router ospfv3 command. If this argument is included, only information for the specified routing process is displayed.
	<i>router-id</i>	(Optional) 32-bit router ID value specified in four-part, dotted-decimal notation.

Defaults No default behavior or value

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	ospf	read

Examples The following is sample output from the **show ospfv3 border-routers** command:

```
RP/0/RP0/CPU0:router# show ospfv3 border-routers
```

```
OSPFv3 1 Internal Routing Table
```

```
Codes: i - Intra-area route, I - Inter-area route
```

```
i 10.0.0.207 [1] via fe80::3034:30ff:fe33:3742, POS 0/3/0/0, ABR/ASBR, Area 1, SPF 3
i 10.0.0.207 [10] via fe80::204:c0ff:fe22:73fe, Ethernet0/0/0/0, ABR/ASBR, Area 0, SPF 7
```

R3.3 Beta Draft – Cisco Confidential Information

Table 97 describes the significant fields shown in the display.

Table 97 *show ospf border-routers Field Descriptions*

Field	Description
i	Type of this route; i indicates an intra-area route, I an inter-area route.
10.0.0.207	Router ID of destination.
[1]	Cost of using this route.
fe80::3034:30ff:fe33:3742	Next hop toward the destination.
POS0/3/0/0	Packets destined for fe80::3034:30ff:fe33:3742 are sent over Packet-over-SONET (POS) interface 3/0/0/0.
ABR/ASBR	Router type of the destination; it is either an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR) or both.
Area 1	Area ID of the area from which this route is learned.
SPF 3	Internal number of the shortest path first (SPF) calculation that installs this route.

Related Commands

Command	Description
router ospfv3	Configures an OSPFv3 routing process.

R3.3 Beta Draft—Cisco Confidential Information

show ospfv3 database

To display lists of information related to the Open Shortest Path First Version 3 (OSPFv3) database for a specific router, use the **show ospfv3 database** command in EXEC mode.

```
show ospfv3 [process-name [area-id]] database

show ospfv3 [process-name [area-id]] database [adv-router [router-id]]

show ospfv3 [process-name [area-id]] database [database-summary]

show ospfv3 [process-name [area-id]] database [external] [link-state-id]

show ospfv3 [process-name [area-id]] database [external] [link-state-id] [adv-router [router-id]]

show ospfv3 [process-name [area-id]] database [external] [link-state-id] [self-originate]

show ospfv3 [process-name [area-id]] database [inter-area prefix] [link-state-id]

show ospfv3 [process-name [area-id]] database [inter-area prefix] [link-state-id] [adv-router
[router-id]]

show ospfv3 [process-name [area-id]] database [inter-area prefix] [link-state-id] [self-originate]

show ospfv3 [process-name [area-id]] database [inter-area router] [link-state-id]

show ospfv3 [process-name [area-id]] database [inter-area router] [link-state-id] [adv-router
[router-id]]

show ospfv3 [process-name [area-id]] database [inter-area router] [link-state-id] [self-originate]

show ospfv3 [process-name [area-id]] database [link] [link-state-id]

show ospfv3 [process-name [area-id]] database [link] [link-state-id] [adv-router [router-id]]

show ospfv3 [process-name [area-id]] database [link] [link-state-id] [self-originate]

show ospfv3 [process-name [area-id]] database [network] [link-state-id]

show ospfv3 [process-name [area-id]] database [network] [link-state-id] [adv-router [router-id]]

show ospfv3 [process-name [area-id]] database [network] [link-state-id] [self-originate]

show ospfv3 [process-name [area-id]] database [nssa-external] [link-state-id]

show ospfv3 [process-name [area-id]] database [nssa-external] [link-state-id] [adv-router
[router-id]]

show ospfv3 [process-name [area-id]] database [nssa-external] [link-state-id] [self-originate]

show ospfv3 [process-name [area-id]] database [prefix] [link-state-id]

show ospfv3 [process-name [area-id]] database [prefix] [link-state-id] [adv-router [router-id]]

show ospfv3 [process-name [area-id]] database [prefix] [self-originate] [link-state-id]

show ospfv3 [process-name [area-id]] database [router] [link-state-id]
```

R3.3 Beta Draft—Cisco Confidential Information

show ospfv3 [*process-name* [*area-id*]] **database** [**router**] [**adv-router** [*router-id*]]

show ospfv3 [*process-name* [*area-id*]] **database** [**router**] [**self-originate**] [*link-state-id*]

show ospfv3 [*process-name* [*area-id*]] **database** [**self-originate**]

show ospfv3 [*process-name* [*area-id*]] **database** [**unknown** [**area** | **as** | **link**]] [*link-state-id*]
[**adv-router** [*router-id*]] [**self-originate**]

Syntax Description

<i>process-name</i>	(Optional) Name that uniquely identifies an OSPFv3 routing process. The process name is defined by the router ospfv3 command. If this argument is included, only information for the specified routing process is displayed.
<i>area-id</i>	(Optional) Area number used to define the particular area.
adv-router [<i>router-id</i>]	(Optional) Displays all link-state advertisements (LSAs) of the specified router.
asbr-summary	(Optional) Displays information only about the Autonomous System Boundary Router (ASBR) summary LSAs.
database-summary	(Optional) Displays how many of each type of LSA are in the database for each area and the total.
external	(Optional) Displays information only about the external LSAs.
self-originate	(Optional) Displays only self-originated LSAs (from the local router).
<i>link-state-id</i>	(Optional) LSA ID that uniquely identifies the LSA. For network LSAs and link LSAs, this ID is the interface ID of the link of the router originating the LSA.
inter-area prefix	(Optional) Displays information only about the interarea prefix LSAs.
inter-area router	(Optional) Displays information only about the interarea router LSAs.
link	(Optional) Displays information only about the link LSAs.
network	(Optional) Displays information only about the network LSAs.
nssa-external	(Optional) Displays information only about the not-so-stubby area (NSSA) external LSAs.
prefix	(Optional) Displays information only about the prefix LSAs.
router	(Optional) Displays information only about the router LSAs.
unknown	(Optional) Displays information only about unknown LSAs.
area	(Optional) Displays information only about the area LSAs.
as	(Optional) Displays information only about the autonomous system LSAs.

Defaults

No default behavior or value

Command Modes

EXEC

R3.3 Beta Draft—Cisco Confidential Information

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The various forms of this command deliver information about different OSPFv3 link-state advertisements.

Task ID

Task ID	Operations
ospf	read

Examples

The following is sample output from the **show ospfv3 database** command with no arguments or keywords:

```
RP/0/RP0/CPU0:router# show ospfv3 database
```

```
OSPFv3 Router with ID (10.0.0.207) (Process ID 1)
```

```
Router Link States (Area 0)
```

ADV Router	Age	Seq#	Fragment ID	Link count	Bits
0.0.0.1	163	0x80000039	0	2	None
10.0.0.206	145	0x80000005	0	1	EB
10.0.0.207	151	0x80000004	0	1	EB
192.168.0.0	163	0x80000039	0	1	None

```
Net Link States (Area 0)
```

ADV Router	Age	Seq#	Link ID	Rtr count
10.0.0.207	152	0x80000002	1	3
192.168.0.0	163	0x80000039	1	2

```
Inter Area Prefix Link States (Area 0)
```

ADV Router	Age	Seq#	Prefix
10.0.0.206	195	0x80000001	3002::/56
10.0.0.207	197	0x80000001	3002::/56
10.0.0.206	195	0x80000001	3002::206/128
10.0.0.207	182	0x80000001	3002::206/128

```
Inter Area Router Link States (Area 0)
```

ADV Router	Age	Seq#	Link ID	Dest RtrID
10.0.0.207	182	0x80000001	167772366	10.0.0.206
10.0.0.206	182	0x80000001	167772367	10.0.0.207

```
Link (Type-8) Link States (Area 0)
```

```
show ospfv3 database
```

R3.3 Beta Draft—Cisco Confidential Information

```

ADV Router      Age      Seq#      Link ID      Interface
0.0.0.1         163      0x80000039 1            Et0/0/0/0
10.0.0.207      202      0x80000001 1            Et0/0/0/0
10.0.0.206      200      0x80000001 2            Et0/0/0/0

Intra Area Prefix Link States (Area 0)

ADV Router      Age      Seq#      Link ID      Ref-lstype  Ref-LSID
192.168.0.0     163      0x80000039 0            0x2002      1
192.168.0.0     163      0x80000039 1            0x2001      0
10.0.0.207      157      0x80000001 1001         0x2002      1

```

Table 98 describes the significant fields shown in the display.

Table 98 *show ospfv3 database Field Descriptions*

Field	Description
ADV Router	ID of advertising router.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Fragment ID	Router LSA fragment ID.
Link count	Number of links described.
Bits	B indicates that the router is an Area Border Router. E indicates that the router is an Autonomous System Boundary Router. V indicates that the router is a virtual link endpoint. W indicates that the router is a wildcard multicast receiver.
Link ID	Unique LSA ID.
Rtr count	Number of routers attached to the link.
Prefix	Prefix of the route being described.
Dest RtrID	Router ID of the router being described.
Interface	Link described by the LSA.
Ref-lstype	LSA type of the LSA being referenced.
Ref-LSID	LSA ID of the LSA being referenced.

The following is sample output from the **show ospfv3 database** command with the **external** keyword:

```

RP/0/RP0/CPU0:router# show ospfv3 database external

OSPFv3 Router with ID (10.0.0.206) (Process ID 1)

Type-5 AS External Link States

LS age: 189
LS Type: AS External Link
Link State ID: 0
Advertising Router: 10.0.0.206
LS Seq Number: 80000002
Checksum: 0xa303
Length: 36
Prefix Address: 2222::
Prefix Length: 56, Options: None
Metric Type: 2 (Larger than any link state path)
Metric: 20

```

R3.3 Beta Draft—Cisco Confidential Information

External Route Tag: 0

Table 99 describes the significant fields shown in the display.

Table 99 *show ospfv3 database external Field Descriptions*

Field	Description
OSPFv3 Router with ID	Router ID number.
Process ID	OSPFv3 process name.
LS age	Link-state age.
LS Type	Link-state type.
Link State ID	Link-state ID.
Advertising Router	ID of Advertising router.
LS Seq Number	Link-state sequence number (detects old or duplicate LSAs).
Checksum	LS checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSA.
Prefix Address	IPv6 address prefix of the route being described.
Prefix Length	Length of the IPv6 address prefix.
Metric Type	External type.
Metric	Link-state metric.
External Route Tag	External route tag, a 32-bit field attached to each external route. This tag is not used by the OSPFv3 protocol itself.

The following is sample output from the **show ospfv3 database** command with the **inter-area prefix** keyword:

```
RP/0/RP0/CPU0:router# show ospfv3 database inter-area prefix

OSPFv3 Router with ID (10.0.0.206) (Process ID 1)

Inter Area Prefix Link States (Area 0)

LS age: 715
LS Type: Inter Area Prefix Links
Link State ID: 0
Advertising Router: 10.0.0.206
LS Seq Number: 80000002
Checksum: 0x3cb5
Length: 36
Metric: 1
Prefix Address: 3002::
Prefix Length: 56, Options: None
```

Table 100 describes the significant fields shown in the display.

Table 100 *show ospfv3 database inter-area prefix Field Descriptions*

Field	Description
OSPFv3 Router with ID	Router ID number.
Process ID	OSPFv3 process name.

R3.3 Beta Draft—Cisco Confidential Information

Table 100 *show ospfv3 database inter-area prefix Field Descriptions (continued)*

Field	Description
LS age	Link-state age.
LS Type	Link-state type.
Link State ID	Link-state ID.
Advertising Router	ID of advertising router.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSA.
Metric	Link-state metric.
Prefix Address	IPv6 prefix of the route being described.
Prefix Length	IPv6 prefix length of the route being described.
Options	LA indicates that the prefix is a local address. MC indicates the prefix is multicast capable. NU indicates that the prefix is not unicast capable. P indicates that the prefix should be propagated at a not-so-stubby area (NSSA) area border.

The following is sample output from the **show ospfv3 database** command with the **inter-area router** keyword:

```
RP/0/RP0/CPU0:router# show ospfv3 database inter-area router
```

```
OSPFv3 Router with ID (10.0.0.206) (Process ID 1)
```

```
Inter Area Router Link States (Area 0)
```

```
LS age: 1522
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Inter Area Router Links
Link State ID: 167772366
Advertising Router: 10.0.0.207
LS Seq Number: 80000002
Checksum: 0xcaae
Length: 32
Metric: 1
Destination Router ID: 10.0.0.206
```

Table 101 describes the significant fields shown in the display.

Table 101 *show ospfv3 database inter-area router Field Descriptions*

Field	Description
OSPFv3 Router with ID	Router ID number.
Process ID	OSPFv3 process name.
LS age	Link-state age.

R3.3 Beta Draft—Cisco Confidential Information

Table 101 *show ospfv3 database inter-area router Field Descriptions (continued)*

Field	Description
Options	Type of service options (Type 0 only): DC—Supports demand circuits. E—Capable of processing external LSAs. MC—Forwards IP multicast. N—Supports Type 7 LSAs. R—Router is active. V6—Include in IPv6 routing calculations.
LS Type	Link-state type.
Link State ID	Link-state ID.
Advertising Router	ID of the advertising router.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA.)
Length	Length (in bytes) of the LSAs.
Metric	Link-state metric.
Destination Router ID	Router ID of the router being described.

The following is sample output from the **show ospfv3 database** command with the **link** keyword:

```
RP/0/RP0/CPU0:router# show ospfv3 database link

      OSPFv3 Router with ID (10.0.0.206) (Process ID 1)

      Link (Type-8) Link States (Area 0)

LS age: 620
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Link-LSA (Interface: Ethernet0/0/0/0)
Link State ID: 1 (Interface ID)
Advertising Router: 10.0.0.207
LS Seq Number: 80000003
Checksum: 0x7235
Length: 56
Router Priority: 1
Link Local Address: fe80::204:c0ff:fe22:73fe
Number of Prefixes: 1
Prefix Address: 7002::
Prefix Length: 56, Options: None
```

Table 102 describes the significant fields shown in the display.

Table 102 *show ospfv3 database link Field Descriptions*

Field	Description
OSPFv3 Router with ID	Router ID number.
Process ID	OSPFv3 process name.
LS age	Link-state age.

R3.3 Beta Draft—Cisco Confidential Information

Table 102 show ospfv3 database link Field Descriptions (continued)

Field	Description
Options	Type of service options (Type 0 only): DC—Supports demand circuits. E—Capable of processing external LSAs. MC—Forwards IP multicast. N—Supports type-7 LSAs. R—Router is active. V6—Include in IPv6 routing calculations.
LS Type	Link-state type.
Link State ID	Link-state ID (Interface ID).
Advertising Router	ID of the advertising router.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSAs.
Router Priority	Interface priority of originating router.
Link Local Address	Link local address of the interface.
Number of Prefixes	Number of prefixes associated with the link.
Prefix Address and Length	List of prefixes associated with the link.
Options	LA indicates that the prefix is a local address. MC indicates that the prefix is multicast capable. NU indicates that the prefix is not unicast capable. P indicates that the prefix should be propagated at an NSSA area border.

The following is sample output from the **show ospfv3 database** command with the **network** keyword:

```
RP/0/RP0/CPU0:router# show ospfv3 database network

      OSPFv3 Router with ID (10.0.0.206) (Process ID 1)

      Net Link States (Area 0)

LS age: 1915
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Network Links
Link State ID: 1 (Interface ID of Designated Router)
Advertising Router: 10.0.0.207
LS Seq Number: 80000004
Checksum: 0x4330
Length: 36
  Attached Router: 10.0.0.207
  Attached Router: 0.0.0.1
  Attached Router: 10.0.0.206
```

R3.3 Beta Draft—Cisco Confidential Information

Table 103 describes the significant fields shown in the display.

Table 103 *show ospfv3 database network Field Descriptions*

Field	Description
OSPFv3 Router with ID	Router ID number.
Process ID 1	OSPFv3 process name.
LS age	Link-state age.
Options	Type of service options (Type 0 only): DC—Supports demand circuits. E—Capable of processing external LSAs. MC—Forwards IP multicast. N—Supports Type 7 LSAs. R—Router is active. V6—Include in IPv6 routing calculations.
LS Type	Link-state type.
Link State ID	Link-state ID of the designated router.
Advertising Router	ID of the advertising router.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSA.
Attached Router	List of routers attached to the network, by router ID.

The following is sample output from the **show ospfv3 database** command with the **prefix** keyword:

```
RP/0/RP0/CPU0:router# show ospfv3 database prefix
```

```
OSPFv3 Router with ID (10.0.0.206) (Process ID 1)
```

```
Intra Area Prefix Link States (Area 1)
```

```
Routing Bit Set on this LSA
LS age: 356
LS Type: Intra-Area-Prefix-LSA
Link State ID: 0
Advertising Router: 10.0.0.206
LS Seq Number: 8000001e
Checksum: 0xcdaa
Length: 44
Referenced LSA Type: 2001
Referenced Link State ID: 0
Referenced Advertising Router: 10.0.0.206
Number of Prefixes: 1
Prefix Address: 8006::
Prefix Length: 56, Options: None, Metric: 1
```

R3.3 Beta Draft—Cisco Confidential Information

Table 104 describes the significant fields shown in the display.

Table 104 *show ospfv3 database prefix Field Descriptions*

Field	Description
OSPFv3 Router with ID	Router ID number.
Process ID 1	OSPFv3 process name.
LS age	Link-state age.
LS Type	Link-state type.
Link State ID	Link-state ID of the designated router.
Advertising Router	ID of the advertising router.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSA.
Referenced LSA Type	Router LSA or network LSA of the prefixes referenced.
Referenced Link State ID	Link-state ID of the router or network LSA.
Referenced Advertising Router	Advertising router of the referenced LSA.
Number of Prefixes	Number of prefixes listed in the LSA.
Prefix Address	Prefix associated with the router or network.
Prefix Length	Length of the prefix.
Options	LA indicates that the prefix is a local address. MC indicates that the prefix is multicast capable. NU indicates that the prefix is not unicast capable. P indicates the prefix should be propagated at an NSSA area border.
Metric	Cost of the prefix.

The following is sample output from the **show ospfv3 database** command with the **router** keyword:

```
RP/0/RP0/CPU0:router# show ospfv3 database router
```

```
OSPFv3 Router with ID (10.0.0.206) (Process ID 1)
```

```
Router Link States (Area 0)
```

```
LS age: 814
Options: (V6-Bit E-Bit R-bit)
LS Type: Router Links
Link State ID: 0
Advertising Router: 0.0.0.1
LS Seq Number: 8000003c
Checksum: 0x51ca
Length: 56
Number of Links: 2
```

```
Link connected to: a Transit Network
Link Metric: 10
Local Interface ID: 1
Neighbor (DR) Interface ID: 1
```

R3.3 Beta Draft—Cisco Confidential Information

```
Neighbor (DR) Router ID: 10.0.0.207

Link connected to: a Transit Network
Link Metric: 10
Local Interface ID: 2
  Neighbor (DR) Interface ID: 1
  Neighbor (DR) Router ID: 10.0.0.0
```

Table 105 describes the significant fields shown in the display.

Table 105 *show ospfv3 database router Field Descriptions*

Field	Description
OSPFv3 Router with ID	Router ID number.
Process ID 1	OSPFv3 process name.
LS age	Link-state age.
Options	Type of service options (Type 0 only): DC—Supports demand circuits. E—Capable of processing external LSAs. MC—Forwards IP multicast. N—Supports Type 7 LSAs. R—Router is active. V6—Include in IPv6 routing calculations.
LS Type	Link-state type.
Link State ID	Link-state ID of the designated router.
Advertising Router	ID of the advertising router.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length (in bytes) of the LSA.
Link connected to	The type of network to which this interface is connected. Values are: • Another Router (point-to-point). • A Transit Network. • A Virtual Link.
Link Metric	OSPF cost of using this link.
Local Interface ID	Number that uniquely identifies an interface on a router.

Related Commands

Command	Description
router ospfv3	Configures an OSPFv3 routing process.

R3.3 Beta Draft—Cisco Confidential Information

show ospfv3 flood-list

To display a list of Open Shortest Path First Version 3 (OSPFv3) link-state advertisements (LSAs) waiting to be flooded over an interface, use the **show ospfv3 flood-list** command in EXEC mode.

show ospfv3 [*process-name*] [*area-id*] **flood-list** *interface-type interface-instance*

Syntax Description

<i>process-name</i>	(Optional) Name that uniquely identifies an OSPFv3 routing process. The process name is defined by the router ospfv3 command. If this argument is included, only information for the specified routing process is displayed.
<i>area-id</i>	(Optional) Area number used to define the particular area.
<i>interface-type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a Route Processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults

No default behavior or value

Command Modes

EXEC

R3.3 Beta Draft—Cisco Confidential Information**Command History**

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show ospfv3 flood-list** command to display OSPFv3 packet pacing.

Task ID

Task ID	Operations
ospf	read

Examples

The following sample output from the **show ospfv3 flood-list** command shows three entries for the OSPFv3 1 process running over Packet-over-SONET (POS) interface 0/3/0/0:

```
RP/0/RP0/CPU0:router# show ospfv3 flood-list POS 0/3/0/0
```

```
Flood Lists for OSPFv3 1
```

```
Interface POS 0/3/0/0, Queue length 3
Link state retransmission due in 24 msec
```

```
Displaying 3 entries from flood list:
```

Type	LS ID	ADV RTR	Seq NO	Age	Checksum
3	0.0.0.199	10.0.0.207	0x80000002	3600	0x00c924
3	0.0.0.200	10.0.0.207	0x80000002	3600	0x008966
4	10.0.0.206	10.0.0.207	0x80000008	0	0x001951

Table 106 describes the significant fields shown in the display.

Table 106 show ospfv3 flood-list Field Descriptions

Field	Description
Interface POS 0/3/0/0	Interface for which information is displayed.
Queue length	Number of LSAs waiting to be flooded.
Link state retransmission due in	Length of time before next link-state transmission.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of LSA.
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	router ospfv3	Configures an OSPFv3 routing process.

R3.3 Beta Draft—Cisco Confidential Information

show ospfv3 interface

To display Open Shortest Path First Version 3 (OSPFv3) interface information, use the **show ospfv3 interface** command in EXEC mode.

show ospfv3 [*process-name*] [*area-id*] **interface** [*interface-type interface-instance*]

Syntax Description	
<i>process-name</i>	(Optional) Name that uniquely identifies an OSPFv3 routing process. The process name is defined by the router ospfv3 command. If this argument is included, only information for the specified routing process is displayed.
<i>area-id</i>	(Optional) Area number used to define the particular area.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a Route Processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults No default behavior or value

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Release	Modification
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show ospfv3 interface** command when the adjacency between two neighboring routers is not forming. Adjacency means that the routers synchronize their databases when they discover each other.

You can look at the output to check the physical link and line protocol status and to confirm that the network type and timer intervals match those of the neighboring routers.

Task ID

Task ID	Operations
ospf	read

Examples

The following is sample output from the **show ospfv3 interface** command when Packet-over-SONET (POS) interface 0/2/0/0 is specified:

```
RP/0/RP0/CPU0:router# show ospfv3 interface POS 0/2/0/0
```

```
POS 0/2/0/0 is up, line protocol is up
  Link Local address fe80::203:a0ff:fe9d:f3fe, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.0.0.206
  Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.0.0.207, local address fe80::204:c0ff:fe22:73fe
  Backup Designated router (ID) 10.0.0.206, local address fe80::203:a0ff:fe9d:f3fe
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 0/2/1, flood queue length 0
  Next 0(0)/0(0)/0(0)
  Last flood scan length is 2, maximum is 9
  Last flood scan time is 0 msec, maximum is 1 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.0.0.207 (Designated Router)
  Suppress hello for 0 neighbor(s)
```

Table 107 describes the significant fields shown in the display.

Table 107 show ospfv3 interface Field Descriptions

Field	Description
POS 0/2/0/0	Status of the physical link and operational status of the protocol.
Link Local Address	Interface link local address and interface ID.
Area	OSPFv3 area ID, process ID, instance ID, and router ID.
Transmit Delay	Transmit delay and interface state.
Designated Router	Designated router ID and respective interface IPv6 address.

R3.3 Beta Draft—Cisco Confidential Information**Table 107** show ospfv3 interface Field Descriptions (continued)

Field	Description
Backup Designated router	Backup designated router ID and respective interface IPv6 address.
Timer intervals configured	Configuration of timer intervals.
Hello	Number of seconds until next hello packet is sent over this interface.
Index 0/2/1	Link, area and autonomous system flood indexes, and number of flood queue entries.
Next 0(0)/0(0)/0(0)	Next link, area and autonomous system flood information, data pointer, and index.
Last flood scan length	Length of last flood scan.
Last flood scan time	Time of last flood scan (in milliseconds).
Neighbor Count	Count of network neighbors and list of adjacent neighbors.
Suppress hello	Count of neighbors suppressing hello messages.

Related Commands

Command	Description
router ospfv3	Configures an OSPFv3 routing process.

R3.3 Beta Draft—Cisco Confidential Information

show ospfv3 neighbor

To display Open Shortest Path First Version 3 (OSPFv3) neighbor information on an individual interface basis, use the **show ospfv3 neighbor** command in EXEC mode.

```
show ospfv3 [process-name] [area-id] neighbor [interface-type interface-instance] [neighbor-id]
[detail]
```

Syntax Description

<i>process-name</i>	(Optional) Name that uniquely identifies an OSPFv3 routing process. The process name is defined by the router ospfv3 command. If this argument is included, only information for the specified routing process is displayed.
<i>area-id</i>	(Optional) Area ID. If you do not specify an area, all areas are displayed.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a Route Processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
<i>neighbor-id</i>	(Optional) Neighbor router ID.
detail	(Optional) Displays all neighbors given in detail (lists all neighbors).

Defaults

No default behavior or value

Command Modes

EXEC

R3.3 Beta Draft—Cisco Confidential Information

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show ospfv3 neighbor** command when the adjacency between two neighboring routers is not forming. Adjacency means that the routers synchronize their databases when they discover each other.

Task ID

Task ID	Operations
ospf	read

Examples

The following is sample output from the **show ospfv3 neighbor** command showing two lines of summary information for each neighbor:

```
RP/0/RP0/CPU0:router# show ospfv3 neighbor
```

```
Neighbors for OSPFv3 1
```

```
Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
10.0.0.207       1     FULL/ -         00:00:35    3             POS 0/3/0/0
    Neighbor is up for 01:08:05
10.0.0.207       1     FULL/DR         00:00:35    2             Ethernet0/0/0/0
    Neighbor is up for 01:08:05
```

```
Total neighbor count: 2
```

[Table 108](#) describes the significant fields shown in the display.

Table 108 *show ospfv3 neighbor Field Descriptions*

Field	Description
ID	Neighbor router ID.
Pri	Router priority for designated router election. A router with a priority of 0 is never elected as the designated router or backup designated router.
State	OSPFv3 state.
Dead Time	Time (in hh:mm:ss) to elapse before OSPFv3 declares the neighbor dead.
Interface ID	Number that uniquely identifies an interface on a router.
Interface	Name of the interface that connects to this neighbor.
Neighbor is up	Time (in hh:mm:ss) that the OSPFv3 neighbor has been up.

R3.3 Beta Draft—Cisco Confidential Information

The following is sample output showing summary information about the neighbor that matches the neighbor ID:

```
RP/0/RP0/CPU0:router# show ospfv3 neighbor 10.0.0.207
```

Neighbors for OSPFv3 1

```
Neighbor 10.0.0.207
  In the area 0 via interface Ethernet0/0/0/0
  Neighbor: interface-id 2, link-local address fe80::204:c0ff:fe22:73fe
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 10.0.0.207 BDR is 10.0.0.206
  Options is 0x13
  Dead timer due in 00:00:38
  Neighbor is up for 01:09:21
  Index 0/1/2, retransmission queue length 0, number of retransmission 1
  First 0(0)/0(0)/0(0) Next 0(0)/0(0)/0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec
```

```
Neighbor 10.0.0.207
  In the area 1 via interface POS 0/3/0/0
  Neighbor: interface-id 3, link-local address fe80::3034:30ff:fe33:3742
  Neighbor priority is 1, State is FULL, 6 state changes
  Options is 0x13
  Dead timer due in 00:00:38
  Neighbor is up for 01:09:21
  Index 0/1/1, retransmission queue length 0, number of retransmission 1
  First 0(0)/0(0)/0(0) Next 0(0)/0(0)/0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec
```

Total neighbor count: 2

Table 109 describes the significant fields shown in the display.

Table 109 *show ospfv3 neighbor 10.0.0.207 Field Descriptions*

Field	Description
Neighbor	Neighbor router ID.
In the area	Area and interface through which the OSPFv3 neighbor is known.
link-local address	Link local address of the interface.
Neighbor priority	Router priority of neighbor and neighbor state.
State	OSPFv3 state.
state changes	Number of state changes for this neighbor.
DR is	Neighbor ID of the designated router.
BDR is	Neighbor ID of the backup designated router.
Options	Hello packet options field contents (E-bit only; possible values are 0 and 2; 2 indicates that area is not a stub; 0 indicates that area is a stub).
Dead timer	Time (in hh:mm:ss) to elapse before OSPFv3 declares the neighbor dead.

R3.3 Beta Draft—Cisco Confidential Information

Table 109 *show ospfv3 neighbor 10.0.0.207 Field Descriptions (continued)*

Field	Description
Neighbor is up	Time (in hh:mm:ss) that OSPFv3 neighbor has been up.
Index	Index and the remaining lines of this command give detailed information about flooding information received from the neighbor.

The following sample output shows the neighbors that match the neighbor ID on the interface when the interface along with the neighbor ID is specified:

```
RP/0/RP0/CPU0:router# show ospfv3 neighbor POS 0/3/0/1 10.0.0.207
```

```
Neighbors for OSPFv3 1
```

```
Neighbor 10.0.0.207
  In the area 0 via interface POS 0/3/0/1
  Neighbor: interface-id 2, link-local address fe80::204:c0ff:fe22:73fe
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 10.0.0.207 BDR is 10.0.0.206
  Options is 0x13
  Dead timer due in 00:00:39
  Neighbor is up for 01:11:21
  Index 0/1/2, retransmission queue length 0, number of retransmission 1
  First 0(0)/0(0)/0(0) Next 0(0)/0(0)/0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec
```

```
Total neighbor count: 1
```

Table 110 describes the significant fields shown in the display.

Table 110 *show ospfv3 neighbor POS 0/3/0/1 10.0.0.207 Field Descriptions*

Field	Description
Neighbor	Neighbor router ID.
In the area	Area and interface through which the OSPFv3 neighbor is known.
link-local address	Link local address of the interface.
Neighbor priority	Router priority of neighbor and neighbor state.
State	OSPFv3 state.
state changes	Number of state changes for this neighbor.
DR is	Neighbor ID of the designated router.
BDR is	Neighbor ID of the backup designated router.
Options	Hello packet options field contents (E-bit only; possible values are 0 and 2; 2 indicates that area is not a stub; 0 indicates that area is a stub).
Dead timer	Time (in hh:mm:ss) to elapse before OSPFv3 declares the neighbor dead.
Neighbor is up	Time (in hh:mm:ss) that OSPFv3 neighbor has been up.
Index	Index and the remaining lines of this command give detailed information about flooding information received from the neighbor.

```
show ospfv3 neighbor
```

R3.3 Beta Draft—Cisco Confidential Information

The following sample output shows all neighbors on the interface when the interface is specified:

```
RP/0/RP0/CPU0:router# show ospfv3 neighbor POS 0/3/0/1
```

```
Neighbors for OSPFv3 1
```

```
Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
10.0.0.207       1     FULL/DR         00:00:37    2             POS 0/3/0/1
    Neighbor is up for 01:12:33
```

```
Total neighbor count: 1
```

Table 111 describes the significant fields shown in the display.

Table 111 *show ospfv3 neighbor POS 0/3/0/1 Field Descriptions*

Field	Description
ID	Neighbor router ID.
Pri	Router priority for designated router election. A router with a priority of 0 is never elected as the designated router or backup designated router.
State	OSPF state.
Dead Time	Time (in hh:mm:ss) to elapse before OSPF declares the neighbor dead.
Interface ID	Number that uniquely identifies an interface on a router.
Interface	Name of the interface that connects to this neighbor.
Neighbor is up	Amount of time (in hh:mm:ss) that the OSPF neighbor has been up.

The following is sample output showing detailed neighbor information for Packet-over-SONET (POS) interface 0/3/0/1:

```
RP/0/RP0/CPU0:router# show ospfv3 neighbor POS 0/3/0/1 detail
```

```
Neighbors for OSPFv3 1
```

```
Neighbor 10.0.0.207
  In the area 0 via interface POS 0/3/0/1
  Neighbor: interface-id 2, link-local address fe80::204:c0ff:fe22:73fe
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 10.0.0.207 BDR is 10.0.0.206
  Options is 0x13
  Dead timer due in 00:00:39
  Neighbor is up for 01:13:40
  Index 0/1/2, retransmission queue length 0, number of retransmission 1
  First 0(0)/0(0)/0(0) Next 0(0)/0(0)/0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec
```

```
Total neighbor count: 1
```


R3.3 Beta Draft—Cisco Confidential Information

Table 112 describes the significant fields shown in the display.

Table 112 *show ospfv3 neighbor POS 0/3/0/1 detail Field Descriptions*

Field	Description
Neighbor	Neighbor router ID.
In the area	Area and interface through which the OSPFv3 neighbor is known.
link-local address	Link local address of the interface.
Neighbor priority	Router priority of neighbor and neighbor state.
State	OSPFv3 state.
state changes	Number of state changes for this neighbor.
DR is	Neighbor ID of the designated router.
BDR is	Neighbor ID of the backup designated router.
Options	Hello packet options field contents (E-bit only; possible values are 0 and 2; 2 indicates that area is not a stub; 0 indicates that area is a stub).
Dead timer	Time (in hh:mm:ss) to elapse before OSPFv3 declares the neighbor dead.
Neighbor is up	Time (in hh:mm:ss) that the OSPFv3 neighbor has been up.
Index	Index and the remaining lines of this command give detailed information about flooding information received from the neighbor.

Related Commands

Command	Description
router ospfv3	Configures an OSPFv3 routing process.

R3.3 Beta Draft—Cisco Confidential Information

show ospfv3 request-list

To display the first ten link-state requests pending that the local router is making to the specified Open Shortest Path First Version 3 (OSPFv3) neighbor and interface, use the **show ospfv3 request-list** command in EXEC mode.

```
show ospfv3 [process-name] [area-id] request-list [interface-type interface-instance]
[neighbor-id]
```

Syntax Description	<i>process-name</i>	(Optional) Name that uniquely identifies an OSPFv3 routing process. The process name is defined by the router ospfv3 command. If this argument is included, only information for the specified routing process is displayed.
	<i>area-id</i>	(Optional) Area ID. If you do not specify an area, all areas are displayed.
	<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
	<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a Route Processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
	<i>neighbor-id</i>	(Optional) Router ID of the OSPFv3 neighbor. This argument must be in 32-bit dotted-decimal notation, similar to an IPv4 address.

Defaults No default behavior or value

Command Modes EXEC

R3.3 Beta Draft—Cisco Confidential Information

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You might use this command when the databases of two neighboring routers are out of synchronization or if the adjacency is not forming between them. Adjacency means that the routers synchronize their databases when they discover each other.

You can look at the list to determine if one router is trying to request a particular database update. Entries that appear to be suspended in the list usually indicate that updates are not being delivered. One possible reason for this behavior is a maximum transmission unit (MTU) mismatch between the routers.

You might also look at this list to make sure it is not corrupted. The list should refer to database entries that actually exist.

Task ID

Task ID	Operations
ospf	read

Examples

The following sample output shows request lists for neighbor 10.0.0.207 on the OSPFv3 1 process:

```
RP/0/RP0/CPU0:router# show ospfv3 1 request-list 10.0.0.207 POS 0/3/0/0
```

Request Lists for OSPFv3 1

Neighbor 10.0.0.207, interface POS 0/3/0/0 address fe80::3034:30ff:fe33:3742

Type	LS ID	ADV RTR	Seq NO	Age	Checksum
1	192.168.58.17	192.168.58.17	0x80000012	12	0x0036f3
2	192.168.58.68	192.168.58.17	0x80000012	12	0x00083f

Table 113 describes the significant fields shown in the display.

Table 113 show ospfv3 request-list Field Descriptions

Field	Description
Neighbor	Router ID of the neighboring router.
interface	Name of the interface that connects to this neighbor.
address	IPv6 address of the neighbor.
Type	Type of link-state advertisement (LSA).
LS ID	Link-state ID of the LSA.
ADV RTR	Router ID of the advertising router.

R3.3 Beta Draft—Cisco Confidential Information

Table 113 *show ospfv3 request-list Field Descriptions (continued)*

Field	Description
Seq NO	Sequence number of the LSA.
Age	Age of the LSA (in seconds).
Checksum	Checksum of the LSA.

Related Commands

Command	Description
router ospfv3	Configures an OSPFv3 routing process.
show ospfv3 retransmission-list	Displays the first ten link-state entries in the retransmission list that the local router sends to the specified neighbor over the specified interface.

R3.3 Beta Draft—Cisco Confidential Information

show ospfv3 retransmission-list

To display the first ten link-state entries in the retransmission list that the local router sends to the specified neighbor over the specified interface, use the **show ospfv3 retransmission-list** command in EXEC mode.

```
show ospfv3 [process-name] [area-id] retransmission-list [interface-type interface-instance]
[neighbor-id]
```

Syntax Description	
<i>process-name</i>	(Optional) Name that uniquely identifies an Open Shortest Path First Version 3 (OSPFv3) routing process. The process name is defined by the router ospfv3 command. If this argument is included, only information for the specified routing process is displayed.
<i>area-id</i>	(Optional) Area ID. If you do not specify an area, all areas are displayed.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash mark between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a Route Processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
<i>neighbor-id</i>	(Optional) IP address of the OSPFv3 neighbor.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.

R3.3 Beta Draft—Cisco Confidential Information

Release	Modification
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You might use this command when the databases of two neighboring routers are out of synchronization or if the adjacency is not forming between them. Adjacency means that the routers synchronize their databases when they discover each other.

You can look at the list to determine if one router is trying to request a particular database update. Entries that appear to be suspended in the list usually indicate that updates are not being delivered. One possible reason for this behavior is a maximum transmission unit (MTU) mismatch between the routers.

You might also look at this list to make sure it is not corrupted. The list should refer to database entries that actually exist.

Task ID

Task ID	Operations
ospf	read

Examples

The following sample output shows the retransmission list for neighbor 10.0.124.4 on Packet-over-SONET (POS) interface 0/3/0/0:

```
RP/0/RP0/CPU0:router# show ospfv3 retransmission-list 10.0.124.4 POS 0/3/0/0
```

```
Neighbor 10.0.124.4, interface POS 0/3/0/0 address fe80::3034:30ff:fe33:3742
```

[Table 114](#) describes the significant fields shown in the display.

Table 114 show ospfv3 retransmission-list 10.0.124.4 POS 0/3/0/0 Field Descriptions

Field	Description
Neighbor	Router ID of the neighboring router.
interface	Name of the interface that connects to this neighbor.
address	IPv6 address of the neighbor.

Related Commands

Command	Description
router ospfv3	Configures an OSPFv3 routing process.
show ospfv3 request-list	Displays the first ten link-state requests pending that the local router is making to the specified neighbor and interface.

R3.3 Beta Draft—Cisco Confidential Information

show ospfv3 routes

To display the Open Shortest Path First Version 3 (OSPFv3) route table, use the **show ospfv3 routes** command in EXEC mode.

show ospfv3 [*process-name*] **routes** [**external** | **connected**] [*ipv6-prefix/prefix-length*]

show ospfv3 [*process-name*] **routes summary**

Syntax Description	
<i>process-name</i>	(Optional) Name that uniquely identifies an OSPFv3 routing process. The process name is defined by the router ospf command. If this argument is included, only information for the specified routing process is displayed.
external	(Optional) Displays routes redistributed from other protocols.
connected	(Optional) Displays connected routes.
<i>ipv6-prefix</i>	(Optional) IP Version 6 (IPv6) prefix, which limits output to a specific route. This argument must be in the form documented in RFC 2373, in which the address is specified in hexadecimal using 16-bit values between colons.
<i>/prefix-length</i>	(Optional) Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value.
summary	Displays a summary of the route table.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

Use the **show ospfv3 routes** command to display the OSPFv3 private routing table (which contains only routes calculated by OSPFv3). If there is something wrong with a route in the Routing Information Base (RIB), check the OSPFv3 copy of the route to determine if it matches the RIB contents. If it does not match, there is a synchronization problem between OSPFv3 and the RIB. If the routes match and the route is incorrect, OSPFv3 has made an error in its routing calculation.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	ospf	read

Examples

The following sample output shows the route table for OSPFv3 process 1:

```
RP/0/RP0/CPU0:router# show ospfv3 1 routes

Route Table for OSPFv3 1 with ID 10.3.4.2

* 3000:11:22::/64, Inter, cost 21/0, area 1
  POS 0/3/0/0, fe80::3034:30ff:fe33:3742
  10.0.0.207/200
* 3000:11:22:1::/64, Inter, cost 31/0, area 1
  POS 0/3/0/0, fe80::3034:30ff:fe33:3742
  10.0.0.207/1
* 3333::/56, Ext2, cost 20/1, P:0 F:0
  POS 0/3/0/0, fe80::3034:30ff:fe33:3742
  10.0.0.207/0
* 6050::/56, Ext2, cost 20/1, P:0 F:0
  POS 0/3/0/0, fe80::3034:30ff:fe33:3742
  10.0.0.207/1
* 7002::/56, Intra, cost 10/0, area 0
  Ethernet0/0/0/0, connected

* 3000:11:22::/64, Inter, cost 21/0, area 1
  POS 0/3/0/0, fe80::3034:30ff:fe33:3742
  10.0.0.207/200
```

Table 115 describes the significant fields in the display.

Table 115 show ospfv3 1 route Field Descriptions

Field	Description
3000:11:22::/64	Prefix to which the local router has a route.
Inter	Prefix 3000:11:22::/64 is interarea.
cost 21/0	Sum of the link costs required to reach prefix 3000:11:22::/64. 0. In this example, 20 is the external cost.
POS 0/3/0/0	Packets destined for prefix 3000:11:22::/64 are sent over the POS 0/3/0/0 interface.
fe80::3034:30ff:fe33:3742	Next-hop router on the path to prefix 3000:11:22::/64.
10.0.0.207	Router 10.0.0.207 is the router that advertised this route.

Related Commands	Command	Description
	router ospfv3	Configures an OSPFv3 routing process.

R3.3 Beta Draft—Cisco Confidential Information

show ospfv3 summary-prefix

To display Open Shortest Path First Version 3 (OSPFv3) aggregated summary address information, use the **show ospfv3 summary-prefix** command in EXEC mode.

show ospfv3 [*process-name*] **summary-prefix**

Syntax Description	<i>process-name</i> (Optional) Name that uniquely identifies an OSPFv3 routing process. The process name is defined by the router ospfv3 command. If this argument is included, only information for the specified routing process is displayed.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the show ospfv3 summary-prefix command if you configured summarization of external routes with the summary-prefix command and you want to display configured summary addresses.

Task ID	Task ID	Operations
	ospf	read

Examples	The following sample output shows the summary prefix address for the OSPFv3 1 process:

```
RP/0/RP0/CPU0:router# show ospfv3 1 summary-prefix
```

```
OSPFv3 Process 1, Summary-prefix
```

```
4004:f000::/32 Metric 20, Type 2, Tag 0
```

R3.3 Beta Draft – Cisco Confidential Information

Table 116 describes the significant fields shown in the display.

Table 116 *show ospfv3 1 summary-prefix Field Descriptions*

Field	Description
4004:f000::/32	Summary prefix designated for a range of IPv6 prefixes. The length of the IPv6 prefix.
Metric	Metric used to advertise the summary routes.
Type	External link-state advertisements (LSAs) metric type.
Tag	Tag value that can be used as a “match” value for controlling redistribution through route maps.

Related Commands

Command	Description
router ospfv3	Configures an OSPFv3 routing process.
summary-prefix (OSPFv3)	Creates aggregate addresses for routes being redistributed from another routing protocol into OSPFv3.

R3.3 Beta Draft—Cisco Confidential Information

show ospfv3 virtual-links

To display parameters and the current state of Open Shortest Path First Version 3 (OSPFv3) virtual links, use the **show ospfv3 virtual-links** command in EXEC mode.

show ospfv3 [*process-name*] **virtual-links**

Syntax Description	<i>process-name</i> (Optional) Name that uniquely identifies an OSPFv3 routing process. The process name is defined by the router ospfv3 command. If this argument is included, only information for the specified routing process is displayed.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

The information displayed in the **show ospfv3 virtual-links** command is useful in debugging OSPFv3 routing operations.

Task ID	Task ID	Operations
	ospf	read

Examples	The following sample output shows the virtual links for the OSPFv3 1 process:

```
RP/0/RP0/CPU0:router# show ospfv3 1 virtual-links
```

```
Virtual Links for OSPFv3 1
Virtual Link to router 172.31.101.2 is up
Interface ID 16, IPv6 address 3002::206
Transit area 0.0.0.1, via interface POS 0/3/0/0, Cost of using 11
Transmit Delay is 5 sec, State POINT_TO_POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

R3.3 Beta Draft—Cisco Confidential Information

Table 117 describes the significant fields shown in the display.

Table 117 *show ospfv3 virtual-links Field Descriptions*

Field	Description
Virtual Link to router 172.31.101.2 is up	Specifies the OSPFv3 neighbor, and if the link to that neighbor is up or down.
Interface ID 16	ID of the virtual link interface.
IPv6 address 3002::206	IPv6 address of virtual link endpoint.
Transit area 0.0.0.1	Transit area through which the virtual link is formed.
via interface POS 0/3/0/0	Interface through which the virtual link is formed.
Cost of using 11	Cost of reaching the OSPF neighbor through the virtual link.
Transmit Delay is 5 sec	Transmit delay on the virtual link.
State POINT_TO_POINT	State of the OSPFv3 neighbor.
Timer intervals	Various timer intervals configured for the link.
Hello due in 0:00:08	When the next hello message is expected from the neighbor (in hh:mm:ss).
Adjacency State FULL	Adjacency state between the neighbors.

Related Commands

Command	Description
router ospfv3	Configures an OSPFv3 routing process.

R3.3 Beta Draft—Cisco Confidential Information

show protocols (OSPFv3)

To display information about the Open Shortest Path First Version 3 (OSPFv3) process running on the router, use the **show protocols** command in EXEC mode.

```
show protocols [afi-all | ipv4 | ipv6] [all | protocol]
```

Syntax Description	
afi-all	(Optional) Specifies all address families.
ipv4	(Optional) Specifies an IPv4 address family.
ipv6	(Optional) Specifies an IPv6 address family.
all	(Optional) Specifies all protocols for a given address family.
<i>protocol</i>	(Optional) Specifies a routing protocol. For the IPv4 address family, the options are: • bgp • isis • ospf For the IPv6 address family, the options are: • bgp • isis • ospfv3

Defaults	Default is IPv4.

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The afi-all keyword was added.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	ospf	read

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example is sample output from the **show protocols** command:

```
RP/0/RP0/CPU0:router# show protocols ipv6 ospfv3
```

```
Routing Protocol OSPFv3 1
  Router Id:10.0.0.1
  Distance:110
  Redistribution:
    None
  Area 0
    POS 0/2/0/2
    Loopback1
```

[Table 118](#) describes the significant fields shown in the display.

Table 118 *show protocols Field Descriptions*

Field	Description
Router Id	Router ID of the OSPFv3 process.
Distance	Administrative distance for the protocol. This distance determines the priority the Routing Information Base (RIB) gives to the routes, as opposed to other protocols, for example, IS-IS.
Redistribution	Protocols from which this OSPFv3 process is redistributing routes.
Area	OSPFv3 areas defined in this process, followed by their associated interfaces.

R3.3 Beta Draft—Cisco Confidential Information**stub (OSPFv3)**

To define an area as a stub area for Open Shortest Path First Version 3 (OSPFv3), use the **stub** command in area configuration mode. To disable this function, use the **no** form of this command.

stub [**no-summary**]

no stub

Syntax Description	no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area. Areas with this option are known as <i>totally stubby</i> areas.

Defaults	No stub area is defined.

Command Modes	Area configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

You must configure the **stub** command on all routers in the stub area. Use the **default-cost** area command on the ABR of a stub area to specify the cost of the default route advertised into the stub area by the ABR.

Two stub area router configuration commands exist: the **stub** and **default-cost** commands. In all routers attached to the stub area, the area should be configured as a stub area using the **stub** command. Use the **default-cost** command only on an ABR attached to the stub area. The **default-cost** command provides the metric for the summary default route generated by the ABR into the stub area.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the **no-summary** keyword on the ABR to prevent it from sending summary LSAs (LSA Type 3) into the stub area.

A stub area does not accept information about routes external to the autonomous system.

Task ID	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to create stub area 5 and specifies a cost of 20 for the default summary route sent into this stub area:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 201
RP/0/RP0/CPU0:router(config-ospfv3)# area 5
RP/0/RP0/CPU0:router(config-ospfv3-ar)# stub
RP/0/RP0/CPU0:router(config-ospfv3-ar)# default-cost 20
```

Related Commands

Command	Description
default-cost (OSPFv3)	Specifies a cost for the default summary route sent into a stub area.

R3.3 Beta Draft—Cisco Confidential Information

summary-prefix (OSPFv3)

To create aggregate addresses for routes being redistributed from another routing protocol into Open Shortest Path First Version 3 (OSPFv3) protocol, use the **summary-prefix** command in router ospfv3 configuration mode. To stop summarizing redistributed routes, use the **no** form of the command.

summary-prefix *ipv6-prefix/prefix-length* [**not-advertise**] [**tag** *tag*]

no summary-prefix *ipv6-prefix/prefix-length*

Syntax Description

<i>ipv6-prefix</i>	Summary prefix designated for a range of IP Version 6 (IPv6) prefixes. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<i>/prefix-length</i>	Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value.
not-advertise	(Optional) Suppresses summary routes that match the address and mask pair from being advertised.
tag <i>tag</i>	(Optional) Specifies a tag value that can be used as a “match” value for controlling redistribution.

Defaults

When this command is not used in router configuration mode, aggregate addresses are not created for routes being redistributed from another routing protocol into the OSPFv3 protocol.

Command Modes

Router ospfv3 configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **summary-prefix** command to cause an OSPFv3 Autonomous System Boundary Router (ASBR) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. This command summarizes only routes from other routing protocols that are being redistributed into OSPFv3.

R3.3 Beta Draft—Cisco Confidential Information

You can use this command multiple times to summarize multiple groups of addresses. The metric used to advertise the summary is the lowest metric of all the more specific routes. This command helps reduce the size of the routing table.

If you want to summarize routes between OSPFv3 areas, use the **range** command.

Task ID

Task ID	Operations
ospf	read, write

Examples

In the following example, if summary prefix 4004:f000:132 is configured and routes 4004:f000:1::/64, 4004:f000:2::/64, and 4004:f000:3::/64 are redistributed into OSPFv3; only route 4004:f000::/32 is advertised in an external link-state advertisement:

```
RP/0/RP0/CPU0:router(config-ospfv3)# summary-prefix 4004:f000::/32
```

Related Commands

Command	Description
range (OSPFv3)	Consolidates and summarizes routes at an area boundary.

R3.3 Beta Draft—Cisco Confidential Information

timers lsa arrival

To set the minimum interval at which the software accepts the same link-state advertisement (LSA) from Open Shortest Path First Version 3 (OSPFv3) neighbors, use the **timers lsa arrival** command in router configuration mode. To restore the default value, use the **no** form of this command.

timers lsa arrival *milliseconds*

no timers lsa arrival

Syntax Description	<i>milliseconds</i>	Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. Range is 0 to 60000 milliseconds.

Defaults	1000 milliseconds

Command Modes	Router ospfv3 configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **timers lsa arrival** command to control the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the LSA is dropped.

We recommend that the *milliseconds* value of the **timers lsa arrival** command be less than or equal to the *hold-interval* value of the **timers throttle lsa all** command for the neighbor.

Task ID	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# timers throttle lsa all 200 10000 45000
RP/0/RP0/CPU0:router(config-ospfv3)# timers lsa arrival 2000
```

Related Commands

Command	Description
timers throttle lsa all (OSPFv3)	Sets rate-limiting values for LSAs being generated.

R3.3 Beta Draft—Cisco Confidential Information

timers pacing flood

To configure link-state advertisement (LSA) flood packet pacing, use the **timers pacing flood** command in router configuration mode. To restore the default flood packet pacing value, use the **no** form of this command.

timers pacing flood *milliseconds*

no timers pacing flood

Syntax Description	<i>milliseconds</i>	Time (in milliseconds) at which LSAs in the flooding queue are paced in between updates. Range is 5 milliseconds to 100 milliseconds.

Defaults	33 milliseconds.

Command Modes	Router ospfv3 configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

Configuring OSPFv3 flood pacing timers allows you to control interpacket spacing between consecutive link-state update packets in the OSPF transmission queue. Use the **timers pacing flood** command to control the rate at which LSA updates occur, thereby preventing high CPU or buffer utilization that can result when an area is flooded with a very large number of LSAs.

The default settings for OSPFv3 packet pacing timers are suitable for the majority of OSPFv3 deployments. Do not change the packet pacing timers unless all other options to meet OSPFv3 packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default flood timers. Furthermore, no guidelines exist for changing timer values; each OSPFv3 deployment is unique and should be considered on a case-by-case basis. The network operator assumes risks associated with changing the default flood timer values.

Task ID	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to configure LSA flood packet-pacing updates to occur in 55-millisecond intervals for OSPFv3 routing process 1:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1  
RP/0/RP0/CPU0:router(config-ospfv3)# timers pacing flood 55
```

Related Commands

Command	Description
show ospfv3	Displays general information about OSPFv3 routing processes.
timers pacing lsa-group	Changes the interval at which OSPFv3 link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged
timers pacing retransmission	Configures LSA retransmission packet pacing.

R3.3 Beta Draft—Cisco Confidential Information

timers pacing lsa-group

To change the interval at which Open Shortest Path First Version 3 (OSPFv3) link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers pacing lsa-group** command in router configuration mode. To restore the default value, use the **no** form of this command.

timers pacing lsa-group *seconds*

no timers pacing lsa-group

Syntax Description	<i>seconds</i>	Interval (in seconds) at which LSAs are grouped and refreshed, checksummed, or aged. Range is 10 to 1800 seconds.

Defaults	<i>seconds</i> : 240 OSPFv3 LSA group pacing is enabled by default.

Command Modes	Router ospfv3 configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

Use the **timers pacing lsa-group** command to control the rate at which LSA updates occur so that high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs can be reduced. The default settings for OSPFv3 packet pacing timers are suitable for the majority of deployments. Do not change the packet pacing timers unless all other options to meet OSPFv3 packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default flooding timers. Furthermore, no guidelines exist for changing timer values; each OSPFv3 deployment is unique and should be considered on a case-by-case basis. The network operator assumes the risks associated with changing the default timer values.

Cisco IOS XR software groups the periodic refresh of LSAs to improve the LSA packing density for the refreshes in large topologies. The group timer controls the interval used for group refreshment of LSAs; however, this timer does not change the frequency that individual LSAs are refreshed (the default refresh rate is every 30 minutes).

R3.3 Beta Draft—Cisco Confidential Information

The duration of the LSA group pacing is inversely proportional to the number of LSAs the router is handling. For example, if you have about 10,000 LSAs, decreasing the pacing interval would benefit you. If you have a very small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might benefit you slightly.

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows how to configure OSPFv3 group packet-pacing updates between LSA groups to occur in 60-second intervals for OSPFv3 routing process 1:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# timers pacing lsa-group 60
```

Related Commands	Command	Description
	show ospfv3	Displays general information about OSPFv3 routing processes.
	timers pacing flood	Configures LSA flood packet pacing.
	timers pacing retransmission	Configures LSA retransmission packet pacing.

R3.3 Beta Draft—Cisco Confidential Information

timers pacing retransmission

To configure link-state advertisement (LSA) retransmission packet pacing, use the **timers pacing retransmission** command in router configuration mode. To restore the default retransmission packet pacing value, use the **no** form of this command.

timers pacing retransmission *milliseconds*

no timers pacing retransmission

Syntax Description	<i>milliseconds</i>	Time (in milliseconds) at which LSAs in the retransmission queue are paced. Range is 5 milliseconds to 200 milliseconds.

Defaults	<i>milliseconds: 66</i>

Command Modes	Router ospfv3 configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **timers pacing retransmission** command to control interpacket spacing between consecutive link-state update packets in the OSPFv3 retransmission queue. This command controls the rate at which LSA updates occur. When an area is flooded with a very large number of LSAs, the LSA updates can result in high CPU or buffer utilization. Using this command reduces CPU or buffer utilization.

The default settings for OSPFv3 packet retransmission pacing timers are suitable for the majority of deployments. Do not change the packet retransmission pacing timers unless all other options to meet OSPFv3 packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default flooding timers. Furthermore, no guidelines exist for changing timer values; each OSPFv3 deployment is unique and should be considered on a case-by-case basis. The network operator assumes risks associated with changing the default packet retransmission pacing timer values.

Task ID	Task ID	Operations
	ospf	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to configure LSA flood pacing updates to occur in 55-millisecond intervals for OSPFv3 routing process 1:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1  
RP/0/RP0/CPU0:router(config-ospfv3)# timers pacing retransmission 55
```

Related Commands

Command	Description
show ospfv3	Displays general information about OSPFv3 routing processes.
timers pacing flood	Configures LSA flood packet pacing.
timers pacing lsa-group	Changes the interval at which OSPFv3 LSAs are collected into a group and refreshed, checksummed, or aged.

R3.3 Beta Draft—Cisco Confidential Information

timers throttle lsa all (OSPFv3)

To set rate-limiting values for Open Shortest Path First Version 3 (OSPFv3) link-state advertisement (LSA) generation, use the **timers throttle lsa all** command in router configuration mode. To restore the default values, use the **no** form of this command.

timers throttle lsa all *start-interval hold-interval max-interval*

no timers throttle lsa all

Syntax Description

<i>start-interval</i>	Minimum delay (in milliseconds) for the generation of LSAs. The first instance of LSA is always generated immediately upon a local OSPFv3 topology change. The generation of the next LSA is not before the start interval. Range is 0 to 600000 milliseconds.
<i>hold-interval</i>	Incremental time (in milliseconds). This value is used to calculate the subsequent rate limiting times for LSA generation. Range is 1 to 600000 milliseconds.
<i>max-interval</i>	Maximum wait time (in milliseconds) between generation of the same LSA. Range is 1 to 600000 milliseconds.

Defaults

start-interval: 500 milliseconds
hold-interval: 5000 milliseconds
max-interval: 5000 milliseconds

Command Modes

Router ospfv3 configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The “same LSA” is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. We recommended that you keep the *milliseconds* value of the **timers lsa arrival** command less than or equal to the *hold-interval* value of the **timers throttle lsa all** command.

Task ID

Task ID	Operations
ospf	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

This example shows how to customize OSPFv3 LSA throttling so that the start interval is 200 milliseconds, the hold interval is 10,000 milliseconds, and the maximum interval is 45,000 milliseconds. The minimum interval between instances of receiving the same LSA is 2000 milliseconds.

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1  
RP/0/RP0/CPU0:router(config-ospfv3)# timers throttle lsa all 200 10000 45000  
RP/0/RP0/CPU0:router(config-ospfv3)# timers lsa arrival 2000
```

Related Commands

Command	Description
show ospfv3	Displays general information about OSPFv3 routing processes.
timers lsa arrival	Sets the minimum interval at which the software accepts the same LSA from OSPFv3 neighbors.

R3.3 Beta Draft—Cisco Confidential Information

timers throttle spf (OSPFv3)

To turn on Open Shortest Path First Version 3 (OSPFv3) shortest path first (SPF) throttling, use the **timers throttle spf** command in router ospfv3 configuration mode. To turn off SPF throttling, use the **no** form of this command.

timers throttle spf *spf-start spf-hold spf-max-wait*

no timers throttle spf *spf-start spf-hold spf-max-wait*

Syntax Description

<i>spf-start</i>	Initial SPF schedule delay (in milliseconds). Range is 1 to 600000 milliseconds.
<i>spf-hold</i>	Minimum hold time (in milliseconds) between two consecutive SPF calculations. Range is 1 to 600000 milliseconds.
<i>spf-max-wait</i>	Maximum wait time (in milliseconds) between two consecutive SPF calculations. Range is 1 to 600000 milliseconds.

Defaults

SPF throttling is not set.

Command Modes

Router ospfv3 configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The first wait interval between SPF calculations is the amount of time (in milliseconds) specified by the *spf-start* argument. Each consecutive wait interval is twice the current hold level (in milliseconds) until the wait time reaches the maximum time (in milliseconds) as specified by the *spf-max-wait* argument. Subsequent wait times remain at the maximum until the values are reset or a link-state advertisement (LSA) is received between SPF calculations.



Tip

Setting a low *spf-start* time and *spf-hold* time causes routing to switch to the alternate path more quickly if a failure occurs. However, it consumes more CPU processing time.

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows how to change the start, hold, and maximum wait interval values to 5, 1000, and 90,000 milliseconds, respectively:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1
RP/0/RP0/CPU0:router(config-ospfv3)# timers throttle spf 5 1000 90000
```

R3.3 Beta Draft—Cisco Confidential Information

transmit-delay (OSPFv3)

To set the estimated time required to send a link-state update packet on the interface, use the **transmit-delay** command. To return to the default value, use the **no** form of this command.

transmit-delay *seconds*

no transmit-delay *seconds*

Syntax Description	<i>seconds</i> Time (in seconds) required to send a link-state update. Range is 1 to 65535 seconds.											
Defaults	1 second											
Command Modes	Process configuration Area configuration Interface configuration Virtual-link configuration											
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>Release 2.0</td><td>This command was introduced on the Cisco CRS-1.</td></tr><tr><td>Release 3.0</td><td>No modification.</td></tr><tr><td>Release 3.2</td><td>This command was supported on the Cisco XR 12000 Series Router.</td></tr><tr><td>Release 3.3</td><td>No modification.</td></tr></table>		Release	Modification	Release 2.0	This command was introduced on the Cisco CRS-1.	Release 3.0	No modification.	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.	Release 3.3	No modification.
Release	Modification											
Release 2.0	This command was introduced on the Cisco CRS-1.											
Release 3.0	No modification.											
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.											
Release 3.3	No modification.											
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the <i>seconds</i> argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface. If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.											
Task ID	<table><tr><th>Task ID</th><th>Operations</th></tr><tr><td>ospf</td><td>read, write</td></tr></table>		Task ID	Operations	ospf	read, write						
Task ID	Operations											
ospf	read, write											

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to configure a transmit delay of 3 seconds for Packet-over-SONET (POS) interface POS 0/3/0/0:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 1  
RP/0/RP0/CPU0:router(config-ospfv3)# area 0  
RP/0/RP0/CPU0:router(config-ospfv3-ar)# interface POS 0/3/0/0  
RP/0/RP0/CPU0:router(config-ospfv3-ar-if)# transmit-delay 3
```

Related Commands

Command	Description
show ospfv3	Displays general information about OSPF routing processes.
virtual-link (OSPFv3)	Sets the estimated time required to send a link-state update packet on the interface.

R3.3 Beta Draft—Cisco Confidential Information

virtual-link (OSPFv3)

To define an Open Shortest Path First Version 3 (OSPFv3) virtual link, use the **virtual-link** command in area configuration mode with the optional parameters. To remove a virtual link, use the **no** form of this command.

virtual-link *router-id*

no virtual-link

Syntax Description

<i>router-id</i>	Router ID associated with the virtual link neighbor. The router ID appears in the show ospfv3 display. This value must be entered in 32-bit dotted-decimal notation, similar to an IP Version 4 (IPv4) address. There is no default.

Defaults

No virtual links are defined.

Command Modes

Area configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

In OSPFv3, when there exists a path through another non-backbone area over which the virtual link can function, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

Virtual links, which are defined in the submode of the area they transit, are in effect virtual point-to-point interfaces belonging to area 0 (the backbone). The virtual links inherit parameter values from the backbone area, rather than the transit area in which they are defined.

Each virtual link neighbor must include the router ID of the virtual link neighbor for the link to be properly established. Use the **show ospfv3** command to display the router ID of an OSPFv3 process.

Use the **virtual-link** command to place the router in virtual-link configuration mode (config-router-ar-vl), from which you can configure virtual-link-specific settings. Commands configured under this mode (such as the **transmit-delay** command) are automatically bound to that virtual link.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	ospf	read, write

Examples

The following example shows how to establish a virtual link with default values for all optional parameters:

```
RP/0/RP0/CPU0:router(config)# router ospfv3 201  
RP/0/RP0/CPU0:router(config-ospfv3)# area 1  
RP/0/RP0/CPU0:router(config-ospfv3-ar)# virtual-link 10.3.4.5
```

Related Commands

Command	Description
show ospfv3	Displays general information about OSPF routing processes.
transmit-delay (OSPFv3)	Sets the estimated time required to send a link-state update packet on the interface.

RIB Commands on Cisco IOS XR Software

Beta Draft Cisco Confidential Information

This chapter describes the commands used to display and clear information in the Routing Information Base (RIB).

For detailed information about RIB concepts, configuration tasks, and examples, see the *Implementing RIB on Cisco IOS XR Software* configuration guide.

R3.3 Beta Draft—Cisco Confidential Information

clear route

To clear routes from the IP routing table, use the **clear route** command in EXEC mode.

clear route [**vrf** *vrf-name*] {**ipv4** | **ipv6** | **afi-all**} {**unicast** | **multicast** | **safi-all**} [*ip-address mask*]

Syntax Description

vrf <i>vrf-name</i>	Specifies a VPN routing and forwarding (VRF) instance.
ipv4	Specifies IP Version 4 address prefixes.
ipv6	Specifies IP Version 6 address prefixes.
afi-all	Specifies IP Version 4 and IP Version 6 address prefixes.
unicast	Specifies unicast address prefixes.
multicast	Specifies multicast address prefixes.
safi-all	Specifies unicast and multicast address prefixes.
<i>ip-address</i>	Network IP address about which routing information should be displayed.
<i>mask</i>	Network mask specified in either of two ways: • Network mask can be a four-part, dotted-decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit is a network address. • Network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are 1s, and the corresponding bits of the address are the network address.

Defaults

If a **vrf** *vrf-name* is not specified, routes are cleared from the default VRF.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The afi-all and safi-all keywords were added.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **clear route** command to clear routes from an IP routing table to a specific network, a matching subnet address, or all routes.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	rib	read, write

Examples	The following example shows how to remove all routes matching the subnet address 192.168.2.0 and mask 255.255.255.0 from the IPv4 unicast routing table: <pre>RP/0/RP0/CPU0:router# clear route ipv4 unicast 192.168.2.0 255.255.255.0</pre> The following example shows how to remove all routes from the IPv4 unicast routing table: <pre>RP/0/RP0/CPU0:router# clear route ipv4 unicast</pre>

Related Commands	Command	Description
	router static	Establishes a static route.
	show route	Displays the current state of the routing table.

R3.3 Beta Draft—Cisco Confidential Information

maximum prefix (RIB)

To set the prefix limit for the VPN routing and forwarding (VRF) instance, use the **maximum prefix** command in global VRF address family configuration mode. To set the prefix limits to the default values, use the **no** form of this command.

maximum prefix *maximum* [*mid-threshold*]

no maximum prefix

Syntax Description	<i>maximum</i>	Maximum number of prefixes allowed in the VRF instance. Range is 2 to 2000000.
	<i>mid-threshold</i>	(Optional) Integer specifying at what percentage of the <i>maximum</i> argument value the software starts to generate a Simple Network Management Protocol (SNMP) trap. Range is 1 to 100.

Command Modes	Global VRF address family configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the maximum prefix command to configure a maximum number of prefixes that a VRF instance is allowed to receive.

Task ID	Task ID	Operations
	rib	read, write

Examples	The following example shows how to set the maximum number of prefixes allowed to 1000:

```
RP/0/RP0/CPU0:router(config)# vrf vrf-A
RP/0/RP0/CPU0:router(config-vrf)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-vrf-af)# maximum prefix 1000
```

Related Commands	Command	Description
	show rib tables	Displays all tables known to the RIB.

R3.3 Beta Draft—Cisco Confidential Information

show rib tables

To display all tables known to the Routing Information Base (RIB), use the **show rib tables** command in EXEC mode.

show rib tables

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

Use the **show rib tables** command to display all tables known to the RIB, including table attributes. Attributes include VPN routing and forwarding (VRF) instance, address family, and maximum prefix information.

Task ID	Task ID	Operations
	rib	read

Examples	The following is sample output from the show rib tables command when entered without an address:

RP/0/RP0/CPU0:router# **show rib tables**

VRF	AFI/SAFI	Table ID	PrfxLmt	PrfxCount	PrfxLmtNotified	FwdRfr
ncd Deleted						
default	ipv4/uni	0xe0000000	2000000	3	No	No
No						
vrf_A	ipv4/uni	0xe0000001	2000000	0	No	No
No						
default	ipv4/multi	0xe0100000	2000000	0	No	No
No						

Table 119 describes the significant fields shown in the display.

R3.3 Beta Draft—Cisco Confidential Information

Table 119 *show rib tables Field Descriptions*

Field	Description
VRF	Name of the VRF instance.
AFI/SAFI	Address family instance.
Table ID	ID of the RIB table.
PrfxLmt	Configured prefix limit for the RIB table.
PrfxCount	Number of configured prefixes in the RIB table.
PrfxLmtNotified	Message sent when prefix limit is exceeded.
FwdRfr	Forward referenced. If No is indicated, a table has been created by RIB because a client has registered for the table, but RIB has not heard from the router space infrastructure (RSI) about the table. RSI manages the tables.

R3.3 Beta Draft—Cisco Confidential Information

show route

To display the current routes in the Routing Information Base (RIB), use the **show route** command in EXEC mode.

```
show route [vrf vrf-name] [afi-all | ipv4 | ipv6] [unicast | multicast | safi-all] [protocol [instance]  
| ip-address mask]
```

Syntax Description	
vrf <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
afi-all	(Optional) Specifies all address families.
ipv4	(Optional) Specifies IP Version 4 address prefixes. This is the default.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
unicast	(Optional) Specifies unicast address prefixes. This is the default.
multicast	(Optional) Specifies multicast address prefixes.
safi-all	(Optional) Specifies unicast and multicast address prefixes.
<i>protocol</i>	(Optional) Name of a routing protocol. If you specify a routing protocol, use one of the following keywords: • bgp • eigrp • isis • ospf • rip
<i>instance</i>	(Optional) Number or name used to identify an instance of the specified protocol.
<i>ip-address</i>	(Optional) Network IP address about which routing information should be displayed.
<i>mask</i>	(Optional) Network mask specified in either of two ways: • Network mask can be a four-part, dotted-decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit is a network address. • Network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are 1s, and the corresponding bits of the address are the network address.

Defaults IPv4 and unicast address prefixes

Command Modes EXEC

R3.3 Beta Draft—Cisco Confidential Information

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The afi-all and safi-all keywords were added.
Release 3.3	The eigrp and rip keywords and vrf vrf-name keyword and argument were added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

When the **afi-all** keyword is used, the *ip-address* and *mask* arguments and **best-local**, **longer-prefixes**, and **next-hop** keywords are not available.

Task ID

Task ID	Operations
rib	read

Examples

The following is sample output from the **show route** command when entered without an address:

```
RP/0/RP0/CPU0:router# show 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, E - EGP
       i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
       U - per-user static route, o - ODR, L - local
```

```
Gateway of last resort is 172.23.54.1 to network 0.0.0.0
```

```
C    10.2.210.0/24 is directly connected, 1d21h, Ethernet0/1/0/0
L    10.2.210.221/32 is directly connected, 1d21h, Ethernet0/1/1/0
C    172.20.16.0/24 is directly connected, 1d21h, ATM4/0.1
L    172.20.16.1/32 is directly connected, 1d21h, ATM4/0.1
C    10.6.100.0/24 is directly connected, 1d21h, Loopback1
L    10.6.200.21/32 is directly connected, 1d21h, Loopback0
S    192.168.40.0/24 [1/0] via 172.20.16.6, 1d21h
```

Table 120 describes the significant fields shown in the display.

Table 120 *show route Field Descriptions*

Field	Description
C	Code indicating how the route was derived. See the code legend preceding the output.
10.2.210.0/24	Address and prefix length of the remote network.
Ethernet0/1/0/0	Specifies the interface through which the specified network can be reached.

R3.3 Beta Draft—Cisco Confidential Information

Table 120 *show route Field Descriptions (continued)*

Field	Description
L	Code indicating how the route was derived. See the code legend preceding the output. In this case, the route was local.
S	Code indicating how the route was derived. See the code legend preceding the output. In this case, the route was derived from a static route.
192.168.40.0/24	Address and prefix length of the remote network connected to the static route.
[1/0]	First number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
via 172.20.16.6	Specifies the address of the next router to the remote network.
1d21h	Specifies the last time the route was updated in days (1d) and hours (21h).

When you specify that you want information about a specific network, more detailed statistics are displayed. The following is sample output from the **show route** command when entered with an IP address:

```
RP/0/RP0/CPU0:router# show route 192.168.11.0

Routing entry for 192.168.11.0/8
  Known via "connected", distance 0, metric 0 (connected)
  Routing Descriptor Blocks:
    192.168.43.5 directly connected, via Ethernet6/0
    Route metric is 0
```

When an Intermediate System-to-Intermediate System (IS-IS) includes an IP address typed length value (TLV) in its link-state packet (LSP) which helps identify the node injecting the route into the network. A loopback address is preferred among interfaces configured under IS-IS. When other networking devices calculate IP routes, they can store the originator IP address with each route in the routing table.

The following example shows the output from the **show route** command for a specific IP address on a router configured with IS-IS. Each path that is shown under the Routing Descriptor Blocks report displays two IP addresses. The first address (10.0.0.9) is the next hop address; the second is the originator IP address from the advertising IS-IS router.

```
RP/0/RP0/CPU0:router# show route 10.0.0.1

Routing entry for 10.0.0.0/8
  Known via "isis", distance 115, metric 10, type level-2
  Installed Jan 22 09:26:56.210
  Routing Descriptor Blocks:
    * 10.0.0.9, from 10.0.0.9, via Ethernet2/1
    Route metric is 10
  No advertising protos.
```

[Table 121](#) describes the significant fields shown when the **show route** command is used with an IP address (previous displays).

Table 121 *show route with IP Address Field Descriptions*

Field	Description
Routing entry for 10.0.0.0/8	Network address and mask.
Known via	Indicates how the route was derived.
distance	Administrative distance of the information source.

R3.3 Beta Draft – Cisco Confidential Information

Table 121 ***show route with IP Address Field Descriptions (continued)***

Field	Description
metric	Route value assigned by the routing protocol.
type	IS-IS type level.
Routing Descriptor Blocks:	Displays the next-hop IP address followed by the information source.
from ... via ...	First address is the next-hop IP address, and the other is the information source. This report is followed by the interface for this route.
Route metric	Best metric for this Routing Descriptor Block.
No advertising protos.	Indicates that no other protocols are advertising the route to their redistribution consumers. If the route is being advertised, protocols are listed in the following manner: Redist Advertisers: isis p ospf 43

Related Commands

Command	Description
router static	Establishes a static route.
show interfaces	Lists interface information.
show route summary	Displays the current contents of the routing table in summary format.

R3.3 Beta Draft—Cisco Confidential Information

show route backup

To display backup routes from the Routing Information Base (RIB), use the **show route backup** command in EXEC mode.

```
show route [vrf vrf-name] [afi-all | ipv4 | ipv6] [unicast | multicast | safi-all] backup [ip-address [mask]]
```

Syntax Description	
vrf <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
afi-all	(Optional) Specifies all address families.
ipv4	(Optional) Specifies IP Version 4 address prefixes.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
safi-all	(Optional) Specifies unicast and multicast address prefixes.
<i>ip-address</i>	(Optional) Network IP address about which backup routing information should be displayed.
<i>mask</i>	(Optional) Network mask specified in either of two ways: • Network mask can be a four-part, dotted decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit is a network address. • Network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are ones, and the corresponding bits of the address are the network address.

Defaults	IPv4 and unicast address prefixes

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The afi-all and safi-all keywords were added.
	Release 3.3	The vrf <i>vrf-name</i> keyword and argument were added.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

R3.3 Beta Draft—Cisco Confidential Information

Use the **show route backup** command to display information about routes that have been installed into the RIB as backup routes. This command also displays information about the currently selected active route for which there is a backup.

When the **afi-all** keyword is used, the *ip-address* and *mask* arguments and **best-local**, **longer-prefixes**, and **next-hop** keywords are not available.

Task ID

Task ID	Operations
rib	read

Examples

The following is sample output from the **show route backup** command:

```
RP/0/RP0/CPU0:router# show route backup
```

```
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, E - EGP
       i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
       U - per-user static route, o - ODR, L - local
S      172.73.51.0/24 is directly connected, 2d20h, POS4/0/0/1
        Backup O E2 [110/1] via 10.12.12.2, POS3/0/0/1
```

Table 122 describes the significant fields shown in the display.

Table 122 *show route backup Field Descriptions*

Field	Description
S	Code indicating how the route was derived. See the legend of the codes preceding the output.
172.73.51.0/24	IP address and length of the route.
2d20h	Time (in hh:mm:ss) since the route was installed in the RIB.
POS4/0/0/1	Outbound interface for the route.
Backup	Identifies the entry as a backup version of the route, typically installed by a different routing protocol.
O	Code indicating how the route was derived. See the code legend preceding the output.

R3.3 Beta Draft—Cisco Confidential Information

Table 122 *show route backup Field Descriptions (continued)*

Field	Description
E2	Code for the type of route. This code is relevant only for OSPF and IS-IS routes. The codes for an OSPF route can be: none—intra-area route IA —interarea route E1—external type 1 E2—external type 2 N1—NSSA external type 1 N2—NSSA external type 2 The codes for an IS-IS route can be: L1—level 1 L2 —level 2 ia —interarea su — summary route
[110/1]	Distance and metric for the route.
10.12.12.2	IP address of next hop on the route.
POS3/0/0/1	Outbound interface for the OSPF version of the route.

Related Commands

Command	Description
show route	Displays the current routes in the RIB.

R3.3 Beta Draft—Cisco Confidential Information

show route best-local

To display the best local address to use for return packets from the given destination, use the **show route best-local** command in EXEC mode.

```
show route [vrf vrf-name] [afi-all | ipv4 | ipv6] [unicast | multicast | safi-all] best-local ip-address
```

Syntax Description

vrf vrf-name	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
afi-all	(Optional) Specifies all address families.
ipv4	(Optional) Specifies IP Version 4 address prefixes.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
safi-all	(Optional) Specifies unicast and multicast address prefixes.
ip-address	IP address about which best local information should be displayed.

Defaults

IPv4 and unicast address prefixes

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The afi-all and safi-all keywords were added.
Release 3.3	The vrf vrf-name keyword and argument were added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show route best-local** command to display information about the best local routes in the routing table.

When the **afi-all** keyword is used, the *ip-address* and *mask* arguments and **best-local**, **longer-prefixes**, and **next-hop** keywords are not available.

Task ID

Task ID	Operations
rib	read

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following is sample output from the **show route best-local** command:

```
RP/0/RP0/CPU0:router# show route best-local 10.12.12.1/32
```

```
Routing entry for 10.12.12.1/32
  Known via "local", distance 0, metric 0 (connected)
  Routing Descriptor Blocks
    10.12.12.1 directly connected, via POS3/0/0/1
    Route metric is 0
```

Table 123 describes the significant fields shown in the display.

Table 123 *show route best-local Field Descriptions*

Field	Description
Routing entry for 10.12.12.1/32	Identifies the requested IP address.
Known via	Indicates how the route was derived.
distance	Administrative distance of the information source.
metric	Route value assigned by the routing protocol.
Routing Descriptor Blocks:	Displays the next-hop IP address followed by the information source.
10.12.12.1 Directly connected ... via ...	First address is the next-hop IP address, followed by a report that it is directly connected. This report is followed by the interface for this route.

Related Commands

Command	Description
show route local	Displays local addresses installed in the RIB as a receive entry.

R3.3 Beta Draft—Cisco Confidential Information

show route connected

To display the current connected routes of the routing table, use the **show route connected** command in EXEC mode.

```
show route [vrf vrf-name] [afi-all | ipv4 | ipv6] [unicast | multicast | safi-all] connected
```

Syntax Description

vrf vrf-name	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
afi-all	(Optional) Specifies all address families.
ipv4	(Optional) Specifies IP Version 4 address prefixes.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
safi-all	(Optional) Specifies unicast and multicast address prefixes.

Defaults

IPv4 and unicast address prefixes

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The afi-all and safi-all keywords were added.
Release 3.3	The vrf vrf-name keyword and argument were added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show route connected** command to display information about connected routes in the routing table.

Task ID

Task ID	Operations
rib	read

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following is sample output from the **show route connected** command:

```
RP/0/RP0/CPU0:router# show route connected
```

```
C    10.2.210.0/24 is directly connected, 1d21h, Ethernet0
C    172.20.16.0/24 is directly connected, 1d21h, ATM4/0.1
C    10.6.100.0/24 is directly connected, 1d21h, Loopback1
```

Table 124 describes the significant fields shown in the display.

Table 124 *show route connected Field Descriptions*

Field	Description
C	Code to indicate the route is connected.
10.2.210.0/24	IP address and length of the route.
1d21h	Time (in hh:mm:ss) since the route was installed in the RIB.
Ethernet0	Outbound interface for the route.

Related Commands

Command	Description
show route summary	Displays the current contents of the RIB.

R3.3 Beta Draft—Cisco Confidential Information

show route local

To display local routes receiving routing updates from the Routing Information Base (RIB), use the **show route local** command in EXEC mode.

```
show route [vrf vrf-name] [afi-all | ipv4 | ipv6] [unicast | multicast | safi-all] local [interface-type
interface-instance]
```

Syntax Description

vrf <i>vrf-name</i>	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
afi-all	(Optional) Specifies all address families.
ipv4	(Optional) Specifies IP Version 4 address prefixes.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
safi-all	(Optional) Specifies unicast and multicast address prefixes.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance as follows: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults

IPv4 and unicast address prefixes

Command Modes

EXEC

R3.3 Beta Draft—Cisco Confidential Information

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The afi-all and safi-all keywords were added.
	Release 3.3	The vrf vrf-name keyword and argument were added.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the show route local command to display information about local routes in the routing table.

Task ID	Task ID	Operations
	rib	read

Examples	The following is sample output from the show route local command:

```
RP/0/RP0/CPU0:router# show route local
```

```
L    10.10.10.1/32 is directly connected, 00:14:36, Loopback0
L    10.91.36.98/32 is directly connected, 00:14:32, POS6/0/0/1
L    172.22.12.1/32 is directly connected, 00:13:35, POS3/0/0/1
L    192.168.20.2/32 is directly connected, 00:13:27, POS4/0/0/1
L    10.254.254.1/32 is directly connected, 00:13:26, POS5/0/0/1
```

Table 125 describes the significant fields shown in the display.

Table 125 *show route local Field Descriptions*

Field	Description
L	Code to indicate the route is local.
10.10.10.1/32	IP address and length of the route.
00:14:36	Time (in hh:mm:ss) since the route was installed in the RIB.
Loopback0	Outbound interface for the route.

Related Commands	Command	Description
	show route connected	Displays information about all clients that have registered with the RIB as protocols.

R3.3 Beta Draft—Cisco Confidential Information

show route longer-prefixes

To display the current routes in the Routing Information Base (RIB) that share a given number of bits with a given network, use the **show route longer-prefixes** command in EXEC mode.

```
show route [vrf vrf-name] [afi-all | ipv4 | ipv6] [unicast | multicast | safi-all] longer-prefixes
            ip-address mask
```

Syntax Description

vrf vrf-name	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
afi-all	(Optional) Specifies all address families.
ipv4	(Optional) Specifies IP Version 4 address prefixes.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
safi-all	(Optional) Specifies unicast and multicast address prefixes.
ip-address	Network IP address about which routing information should be displayed.
mask	Network mask specified in either of two ways: • Network mask can be a four-part, dotted-decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit is a network address. • Network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are 1s, and the corresponding bits of the address are the network address.

Defaults

IPv4 and unicast address prefixes

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The afi-all and safi-all keywords were added.
Release 3.3	The vrf vrf-name keyword and argument were added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show route longer-prefixes** command to troubleshoot forwarding problems whose cause may be a long prefix.

R3.3 Beta Draft—Cisco Confidential Information

When the **afi-all** keyword is used, the *ip-address* and *mask* arguments and **best-local**, **longer-prefixes**, and **next-hop** keywords are not available.

Task ID	Task ID	Operations
	rib	read

Examples

The following is sample output from the **show route longer-prefixes** command:

```
RP/0/RP0/CPU0:router# show route ipv4 172.16.0.0/8 longer-prefixes
```

```
S    172.16.2.0/32 is directly connected, 00:00:24, Loopback0
S    172.16.3.0/32 is directly connected, 00:00:24, Loopback0
S    172.16.4.0/32 is directly connected, 00:00:24, Loopback0
S    172.16.5.0/32 is directly connected, 00:00:24, Loopback0
S    172.16.6.0/32 is directly connected, 00:00:24, Loopback0
S    172.16.7.0/32 is directly connected, 00:00:24, Loopback0
S    172.16.8.0/32 is directly connected, 00:00:24, Loopback0
S    172.16.9.0/32 is directly connected, 00:00:24, Loopback0
```

Table 126 describes the significant fields shown in the display.

Table 126 *show route ipv4 172.16.0.0/8 longer-prefixes Field Descriptions*

Field	Description
S	Code indicating how the route was derived. See the code legend preceding the output.
172.16.2.0/32	IP address and length of the route.
00:00:24	Time (in hh:mm:ss) since the route was installed in the RIB.
Loopback0	Outbound interface for the route.

Related Commands	Command	Description
	router static	Establishes a static route.
	show interfaces	Lists interface information.
	show route summary	Displays the current contents of the routing table in summary format.

R3.3 Beta Draft—Cisco Confidential Information

show route next-hop

To display the next hop gateway or host to a destination address, use the **show route next-hop** command in EXEC mode.

```
show route [vrf vrf-name] [afi-all | ipv4 | ipv6] [unicast | multicast | safi-all] next-hop ip-address
```

Syntax Description

vrf vrf-name	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
afi-all	(Optional) Specifies all address families.
ipv4	(Optional) Specifies IP Version 4 address prefixes.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
safi-all	(Optional) Specifies unicast and multicast address prefixes.
ip-address	IP address about which next hop information is to be displayed.

Defaults

IPv4 and unicast address prefixes

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The afi-all and safi-all keywords were added.
Release 3.3	The vrf vrf-name keyword and argument were added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show route next-hop** command to perform a recursive route lookup on the supplied destination address and return information on the next immediate router (next hop) to the destination.

When the **afi-all** keyword is used, the *ip-address* and *mask* arguments and **best-local**, **longer-prefixes**, and **next-hop** keywords are not available.

Task ID

Task ID	Operations
rib	read

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following is sample output from the **show route next-hop** command:

```
RP/0/RP0/CPU0:router# show route next-hop 10.0.0.1

Routing entry for 10.0.0.0/24
  Known via "connected", distance 0, metric 0 (connected)
  Routing Descriptor Blocks
    10.0.0.50 directly connected, via POS3/0/0/1
    Route metric is 0
```

[Table 127](#) describes the significant fields shown in the display.

Table 127 *show route next-hop Field Descriptions*

Field	Description
Known via	Name of the routing protocol that installed the matching route.
10.0.0.50	IP address of the route.
POS3/0/0/1	Outbound interface for the route.
Route metric is	Metric of the route.

Related Commands

Command	Description
show route	Displays the current contents of the routing table.

R3.3 Beta Draft—Cisco Confidential Information

show route static

To display the current static routes of the Routing Information Base (RIB), use the **show route static** command in EXEC mode.

```
show route [vrf vrf-name] [afi-all | ipv4 | ipv6] [unicast | multicast | safi-all] static
```

Syntax Description

vrf vrf-name	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
afi-all	(Optional) Specifies all address families.
ipv4	(Optional) Specifies IP Version 4 address prefixes.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
safi-all	(Optional) Specifies unicast and multicast address prefixes.

Defaults

IPv4 and unicast address prefixes

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The afi-all and safi-all keywords were added.
Release 3.3	The vrf vrf-name keyword and argument were added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show route static** command to display information about static routes in the routing table.

Task ID

Task ID	Operations
rib	read

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following is sample output from the **show route static** command:

```
RP/0/RP0/CPU0:router# show route static
```

```
S    10.1.1.0/24 is directly connected, 00:54:05, POS3/0/0/1
S    192.168.99.99/32 [1/0] via 10.12.12.2, 00:54:04
```

Table 128 describes the significant fields shown in the display.

Table 128 *show route static Field Descriptions*

Field	Description
S	Code to indicate the route is static.
10.1.1.0/24	IP address and distance for the route.
00:54:05	Time (in hh:mm:ss) since the route was installed in the RIB.
POS3/0/0/1	Outbound interface for the route.
[1/0]	Distance and metric for the route.

Related Commands

Command	Description
show route	Displays the current contents of the routing table.

R3.3 Beta Draft—Cisco Confidential Information

show route summary

To display the current contents of the Routing Information Base (RIB), use the **show route summary** command in EXEC mode.

```
show route [vrf vrf-name] [afi-all | ipv4 | ipv6] [unicast | multicast | safi-all] summary [detail]
```

Syntax Description

vrf vrf-name	(Optional) Specifies a VPN routing and forwarding (VRF) instance.
afi-all	(Optional) Specifies all address families.
ipv4	(Optional) Specifies IP Version 4 address prefixes.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
safi-all	(Optional) Specifies unicast and multicast address prefixes.
detail	(Optional) Displays a detailed summary of the contents of the RIB, including the number of paths and some protocol-specific route attributes.

Defaults

IPv4 and unicast address prefixes

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The afi-all and safi-all keywords were added.
Release 3.3	The vrf vrf-name keyword and argument were added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show route summary** command to display information about routes in the routing information base.

When a route summary is needed frequently—for instance, in a polling manner—use the **show route summary** command without the **detail** keyword. The **detail** keyword is used less frequently for verification purposes because it is much more expensive (in bandwidth), requiring a scan of the entire routing database.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	rib	read

Examples

The following is sample output from the **show route summary** command:

```
RP/0/RP0/CPU0:router# show route summary
```

Route Source	Routes	Backup	Deleted	Memory (bytes)
static	1	0	0	136
connected	2	1	0	408
local	3	0	0	408
ospf	1673	2	0	272
isis	2	0	0	272
Total	10	1	0	1496

The following is sample output from the **show route summary** command with the **detail** keyword:

```
RP/0/RP0/CPU0:router# show route summary detail
```

Route Source	Active Route	Active Path	Backup Route	Backup Path
static	1	1	0	0
connected	2	2	1	1
local	3	3	0	0
isis	1	1	1	1
Level 1:	0	0	1	1
Level 2:	1	1	0	0
ospf 1673	6	12	0	0
Intra-Area:	3	6	0	0
Inter-Area:	3	6	0	0
External-1:	0	0	0	0
External-2:	0	0	0	0
bgp 100	10	20	4	8
External:	5	10	4	8
Internal:	5	10	0	0
local:	0	0	0	0
Total	7	7	2	2

Table 129 describes the significant fields shown in the display.

Table 129 *show route summary Field Descriptions*

Field	Description
Route Source	Routing protocol name.
Routes	Number of selected routes that are present in the routing table for each route source.
Backup	Number of routes that are not selected (are backup to a selected route).
Deleted	Number of routes that have been marked for deletion in the RIB, but have not yet been purged.
Memory	Number of bytes allocated to maintain all routes for the particular route source.

Related Commands

Command	Description
show route	Displays the current contents of the routing table.

R3.3 Beta Draft—Cisco Confidential Information

show route vrf

To display the VPN routing and forwarding (VRF) instance information, use the **show route vrf** command in EXEC mode.

show route vrf *vrf-name* [**afi-all** | **ipv4** | **ipv6**] [**unicast** | **multicast** | **safi-all**] [**summary**] [**detail**]

Syntax Description

<i>vrf-name</i>	Name of the VRF.
afi-all	(Optional) Specifies all address families.
ipv4	(Optional) Specifies IP Version 4 address prefixes.
ipv6	(Optional) Specifies IP Version 6 address prefixes.
unicast	(Optional) Specifies unicast address prefixes.
multicast	(Optional) Specifies multicast address prefixes.
safi-all	(Optional) Specifies unicast and multicast address prefixes.
summary	(Optional) Specifies a summary of the routes.
detail	(Optional) Displays a detailed summary of the VRF table.

Defaults

IPv4 and unicast address prefixes

Command Modes

EXEC

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show route vrf** command to display information about routes in the VRF instance.

Task ID

Task ID	Operations
rib	read

Examples

The following is sample output from the **show route vrf** command:

```
RP/0/RP0/CPU0:router# show route vrf vrf-A
```

TBD

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	show route	Displays the current contents of the routing table.

R3.3 Beta Draft – Cisco Confidential Information

RIP Commands on Cisco IOS XR Software

Beta Draft Cisco Confidential Information

This chapter describes the commands used to configure and monitor the Routing Information Protocol (RIP).

For detailed information about RIP concepts, configuration tasks, and examples, refer to the *Implementing RIP on Cisco IOS XR Software* configuration guide.

R3.3 Beta Draft—Cisco Confidential Information

auto-summary

To enable the automatic summarization of subnet routes into network-level routes, use the **auto-summary** command in the appropriate configuration mode. To disable this function 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.

Defaults	Disabled

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **auto-summary** command to turn on route summarization. Route summarization reduces the amount of routing information in the routing tables.

Disable automatic summarization if you must perform routing between disconnected subnets. When automatic summarization is off, subnets are advertised. Automatic summarization is disabled by default.

Task ID	Task ID	Operations
	rip	read, write

Examples	The following example shows how to turn on RIP auto-summarization:

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)# auto-summary
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	vrf (RIP)	Defines a VRF instance and enters VRF configuration mode.

R3.3 Beta Draft—Cisco Confidential Information

broadcast-for-v2

To send Routing Information Protocol (RIP) Version 2 output packets to a broadcast address, use the **broadcast-for-v2** command in the appropriate configuration mode. To disable this feature, use the **no** form of this command.

broadcast-for-v2

no broadcast-for-v2

Syntax Description This command has no arguments or keywords.

Defaults RIPv2 output packets are not broadcasted.

Command Modes Router configuration
VRF configuration
Interface configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **broadcast-for-v2** command to broadcast RIP Version 2 broadcast updates to hosts that do not listen to multicasts. Version 2 updates (requests and responses) will be sent to the IP broadcast address 255.255.255.255 instead of the IP multicast address 244.0.0.9.

Task ID	Task ID	Operations
	rip	read, write

Examples The following example shows how to send RIP v2 output messages to a broadcast address for all RIP interfaces:

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)# broadcast-for-v2
```

R3.3 Beta Draft—Cisco Confidential Information

clear rip

To clear VRF and interface-related information for Routing Information Protocol (RIP) such as database entries and statistics, use the **clear rip** command in EXEC mode.

clear rip [**vrf** {*vrf* | **all**}]

Syntax Description	vrf { <i>vrf</i> all }	(Optional) Specifies a particular VPN routing and forwarding (VRF) instance or all VRF instances.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

RIP VRFs and interfaces that are forcibly deactivated by the software because of a severe memory state are not activated again until after out-of-memory state is cleared by using the **clear rip**, **clear rip interface** or **clear rip out-of-memory** command.

Task ID	Task ID	Operations
	rip	read

Examples	The following example shows how to clear all database, interface, and VRF entries from the RIP topology table:

RP/0/RP0/CPU0:router# **clear rip vrf all**

Related Commands	Command	Description
	clear rip interface	Clears interface-related information for RIP such as database entries and statistics.
	clear rip out-of-memory	Clears the out-of-memory state for RIP.

R3.3 Beta Draft—Cisco Confidential Information

clear rip database

To clear only database entries from the Routing Information Protocol (RIP) topology table, use the **clear rip database** command in EXEC mode.

clear rip [**vrf** {*vrf* | **all**}] **database** [**interface** *type instance*]

Syntax Description

vrf { <i>vrf</i> all }	(Optional) Specifies a particular VPN routing and forwarding (VRF) instance or all VRF instances.
interface	(Optional) Specifies the interface to clear topology entries.
<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>instance</i>	(Optional) Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	rip	read, write

Examples

The following example shows how to clear only database entries from the topology table for the Packet-over-SONET/SDH (POS) 0/1/0/0 interface:

```
RP/0/RP0/CPU0:router# clear rip database interface pos 0/1/0/0
```

Related Commands

Command	Description
show rip statistics	Displays database and interface entry information for the RIP process.

R3.3 Beta Draft—Cisco Confidential Information

clear rip interface

To clear interface-related information for Routing Information Protocol (RIP) such as database entries and statistics, use the **clear rip interface** command in EXEC mode.

clear rip [**vrf** {*vrf* | **all**}] **interface** *type instance*

Syntax Description

vrf { <i>vrf</i> all }	(Optional) Specifies a particular VPN routing and forwarding (VRF) instance or all VRF instances.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

RIP VRFs and interfaces that are forcibly deactivated by the software because of a severe memory state are not activated again until after out-of-memory state is cleared by using the **clear rip**, **clear rip interface** or **clear rip out-of-memory** command.

Task ID

Task ID	Operations
rip	read, write

Examples

The following example shows how to clear all interface-related data such as routes and statistics from the Packet-over-SONET/SDH (POS)0/1/0/0 interface:

```
RP/0/RP0/CPU0:router# clear rip vrf vpn-1 interface pos 0/1/0/0
```

Related Commands

Command	Description
clear rip	Clears VRF and interface-related information for RIP such as database entries and statistics.
clear rip out-of-memory	Clears the out-of-memory state for RIP.

R3.3 Beta Draft—Cisco Confidential Information

clear rip out-of-memory

To clear the out-of-memory state for Routing Information Protocol (RIP), use the **clear rip out-of-memory** command in EXEC mode.

clear rip [**vrf** {*vrf* | **all**}] **out-of-memory** [**interface** *type instance*]

Syntax Description	vrf { <i>vrf</i> all }	(Optional) Specifies a particular VPN routing and forwarding (VRF) instance or all VRF instances.
	interface	(Optional) Specifies the interface to clear topology entries.
	<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
	<i>instance</i>	(Optional) Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **clear out-of-memory** command, to clear the out-of-memory state completely and allow the RIP process to force the VRF or interface to shut down, if needed.

R3.3 Beta Draft – Cisco Confidential Information

When the router begins to run out of memory, the RIP process can transition through different memory states defined as Normal, Minor, Severe and Critical:

- In Normal state, RIP VRFs and interfaces function normally.
- In Minor state, RIP VRFs and interfaces that are currently active are allowed to remain active. VRFs and interfaces that are not currently active are not allowed to become active until the RIP process transitions to Normal state.
- In Severe state, a few VRFs and interfaces are forcibly brought down periodically until the RIP process transitions to another state.
- In Critical state, the RIP process is forcibly shut down.

VRFs and interfaces that are forcibly shut down in Severe state are not automatically activated when the RIP process transitions to Minor or Normal state. When a VRF or interface is forcibly brought down while in Severe state; the **clear rip**, **clear rip interface** or **clear rip out-of-memory** command clears the Forced Down state and reactivates the VRF or interface.

The **show rip** and **show rip interface** commands allow you to view the current out-of-memory state.

Task ID	Task ID	Operations
	rip	read, write

Examples	The following example shows how to clear the out-of-memory state for a RIP process: RP/0/RP0/CPU0:router# clear out-of-memory

Related Commands	clear rip	Clears VRF and interface-related information for RIP such as database entries and statistics.
	clear rip interface	Clears interface-related information for RIP such as database entries and statistics.
	show rip	Displays all database and interface entry information from the RIP topology table.
	show rip interface	Displays interface entry information from the RIP topology table.

R3.3 Beta Draft—Cisco Confidential Information

clear rip statistics

To clear the Routing Information Protocol (RIP) statistics, use the **clear rip statistics** command in EXEC mode.

clear rip [*vrf {vrf | all}*] **statistics** [*interface type instance*]

Syntax Description	<table> <tr> <td data-bbox="386 491 662 520">vrf {vrf all}</td><td data-bbox="672 491 1520 554">(Optional) Specifies a particular VPN routing and forwarding (VRF) instance or all VRF instances.</td></tr> <tr> <td data-bbox="386 562 662 592">interface</td><td data-bbox="672 562 1520 592">(Optional) Specifies the interface to clear topology entries.</td></tr> <tr> <td data-bbox="386 600 662 630"><i>type</i></td><td data-bbox="672 600 1520 663">(Optional) Interface type. For more information, use the question mark (?) online help function.</td></tr> <tr> <td data-bbox="386 672 662 701"><i>instance</i></td><td data-bbox="672 672 1520 1180"> (Optional) Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function. </td></tr> </table>	vrf {vrf all}	(Optional) Specifies a particular VPN routing and forwarding (VRF) instance or all VRF instances.	interface	(Optional) Specifies the interface to clear topology entries.	<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.	<i>instance</i>	(Optional) Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
vrf {vrf all}	(Optional) Specifies a particular VPN routing and forwarding (VRF) instance or all VRF instances.								
interface	(Optional) Specifies the interface to clear topology entries.								
<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.								
<i>instance</i>	(Optional) Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.								

Defaults	No default behavior or values

Command Modes	EXEC

Command History	<table> <tr> <th data-bbox="386 1491 662 1520">Release</th><th data-bbox="672 1491 1520 1520">Modification</th></tr> <tr> <td data-bbox="386 1528 662 1558">Release 3.3</td><td data-bbox="672 1528 1520 1598">This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.</td></tr> </table>	Release	Modification	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release	Modification				
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.				

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .



R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	rip	read, write

Examples

The following example shows how to clear all RIP statistics:

```
RP/0/RP0/CPU0:router# clear rip statistics
```

Related Commands

Command	Description
show rip statistics	Displays database and interface entry information for the RIP process.

R3.3 Beta Draft—Cisco Confidential Information

default-information originate (RIP)

To generate a default route into Routing Information Protocol (RIP), use the **default-information originate** command in the appropriate configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [*route-policy name*]

no default-information originate

Syntax Description	route-policy name	Route policy to specify criteria for the default route.

Defaults	This command is disabled by default.

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	rip	read, write

Examples	The following example shows how to originate a default route in RIP updates based on the result of running the route policy on the routing table:

```
RP/0/RP0/CPU0:router(config)# router rip  
RP/0/RP0/CPU0:router(config-rip)# default-information originate route-policy policy1
```

Related Commands	Command	Description
	route-policy (RIP)	Applies a routing policy to updates advertised to or received from a RIP neighbor.

R3.3 Beta Draft—Cisco Confidential Information

default-metric (RIP)

To set default metric values for routes redistributed from other protocols into Routing Information Protocol (RIP), use the **default-metric** command in the appropriate configuration mode. To return to the default state, use the **no** form of this command.

default-metric *number-value*

no default-metric

Syntax Description

<i>number-value</i>	Default metric value.

Defaults

Default metrics are not set.

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **default-metric** command with the **redistribute** command to cause RIP to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics by providing a reasonable substitute and enables redistribution to proceed. If you want to set different metrics for other redistributed protocols, use the **route-policy** option in the **redistribute** command.

Task ID

Task ID	Operations
rip	read, write

Examples

The following example shows how a router in autonomous system 109 uses both the RIP and the Open Shortest Path First (OSPF) routing protocols. The example advertises OSPF-derived routes using RIP and assigns the OSPF-derived routes a RIP metric of 10:

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)# vrf vpn-1
RP/0/RP0/CPU0:router(config-rip-vrf)# default-metric 10
RP/0/RP0/CPU0:router(config-rip-vrf)# redistribute ospf 109
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	redistribute (RIP)	Redistributes routes from one routing domain into RIP.

R3.3 Beta Draft—Cisco Confidential Information

distance (RIP)

To define the administrative distance assigned to routes discovered by the Routing Information Protocol (RIP) protocol, use the **distance admin-distance** command in the appropriate configuration mode. To remove the distance definition from the configuration file and restore the system to its default condition, use the **no** form of this command.

distance *admin-distance* [*prefix/length* | *ip-address mask*]

no distance *admin-distance*

Syntax Description		
<i>admin-distance</i>		Administrative distance to be assigned to RIP routes. Range is 0 to 255.
<i>prefix-length</i>		(Optional) The <i>prefix-length</i> argument specifies the length of the IP prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash between must precede the decimal value. Range is 0 to 32 for IPv4 addresses.
<i>ip-address</i>		(Optional) Network IP address about which routing information should be displayed.
<i>mask</i>		(Optional) Network mask specified in either of two ways: • Network mask can be a four-part, dotted decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit is a network address. • Network mask can be indicated as a slash (/) and number. For example, /8 shows that the first 8 bits of the mask are ones, and the corresponding bits of the address are the network address.

Defaults	<i>admin-distance</i> : 120

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **distance** command to change the preference of RIP routes over other protocol routes. When administrative distance and redistribution features are used together, routing behavior may be affected for routes accepted from and advertised to RIP neighbors.

R3.3 Beta Draft—Cisco Confidential Information

Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means that the routing information source cannot be trusted at all and should be ignored.

The order in which you enter distance commands can affect the assigned administrative distances in unexpected ways.

Task ID	Task ID	Operations
	rip	read, write

Examples

The following example shows how to set the administrative distance for a particular prefix:

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)# distance 85 192.168.10.0/24
```

Related Commands

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

R3.3 Beta Draft—Cisco Confidential Information

interface (RIP)

To define the interfaces on which the Routing Information Protocol (RIP) protocol runs, use the **interface** command in router configuration mode. To disable RIP routing for interfaces, use the **no** form of this command.

interface *type instance*

no interface *type instance*

Syntax Description	<table> <tr> <td data-bbox="342 575 602 646"><i>type</i></td><td data-bbox="602 575 1502 646">Interface type. For more information, use the question mark (?) online help function.</td></tr> <tr> <td data-bbox="342 646 602 1136"><i>instance</i></td><td data-bbox="602 646 1502 1136"> Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function. </td></tr> </table>	<i>type</i>	Interface type. For more information, use the question mark (?) online help function.	<i>instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
<i>type</i>	Interface type. For more information, use the question mark (?) online help function.				
<i>instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.				
Defaults	When you do not specify this command in configuration mode, RIP routing for interfaces is not enabled.				
Command Modes	Router configuration VRF configuration				
Command History	<table> <tr> <th data-bbox="342 1465 602 1505">Release</th><th data-bbox="602 1465 1502 1505">Modification</th></tr> <tr> <td data-bbox="342 1505 602 1581">Release 3.3</td><td data-bbox="602 1505 1502 1581">This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.</td></tr> </table>	Release	Modification	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release	Modification				
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.				
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the interface command to associate a specific interface with a RIP process. The interface remains associated with the process even when the IPv4 address of the interface changes.				

R3.3 Beta Draft—Cisco Confidential Information

This command places the router in interface configuration mode, from which you can configure interface-specific settings. Commands configured under this mode (such as the **broadcast-for-v2** command) are automatically bound to that interface.

Task ID	Task ID	Operations
	rip	read, write

Examples

The following example shows how to enter interface configuration mode for a RIP process, and send RIP Version 2 messages to the broadcast address on the Packet-over-SONET/SDH (POS) interface 0/1/0/0:

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)# interface POS 0/1/0/0
RP/0/RP0/CPU0:router(config-rip-if)# broadcast-for-v2
```

Related Commands	Command	Description
	broadcast-for-v2	Sends RIP Version 2 output packets to a broadcast address.

R3.3 Beta Draft—Cisco Confidential Information

maximum-paths (RIP)

To configure the maximum number of parallel routes that the Routing Information Protocol (RIP) protocol will install into the routing table, use the **maximum-paths** command in the appropriate configuration mode. To remove the **maximum-paths** command from the configuration file and restore the system to its default condition with respect to RIP, use the **no** form of this command.

maximum-paths *maximum*

no maximum-paths

Syntax Description

<i>maximum</i>	Maximum number of parallel routes that RIP can install in a routing table. Range is 1 to 32 for Cisco CRS-1 routers and 1 to 16 for Cisco XR 12000 Series Routers.

Defaults

<i>maximum</i> (Cisco CRS-1): 4 routes
<i>maximum</i> (Cisco XR 12000 Series Router): 4 routes

Command Modes

Router configuration
VRF configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
rip	read, write

Examples

The following example shows how to allow a maximum of 16 paths to a destination:

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)# maximum-paths 16
```

R3.3 Beta Draft – Cisco Confidential Information

metric-zero-accept

To allow RIP to accept routing entries from RIP updates with a metric set to zero (0), use the **metric-zero-accept** command in interface configuration mode. To remove the **metric-zero-accept** command from the configuration file and restore the system to its default condition with respect to RIP, use the **no** form of this command.

metric-zero-accept

no metric-zero-accept

Syntax Description	This command has no arguments or keywords.

Defaults	Metric zero is not set.

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. After the metric-zero-accept command is configured on routing entries from RIP updates, RIP accepts these routes and then sets the metric to one (1).

Task ID	Task ID	Operations
	rip	read, write

Examples	The following example shows how to set the RIP interface to accept metric zero on routing entries:

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-rip-if)# metric-zero-accept
```

R3.3 Beta Draft—Cisco Confidential Information

neighbor (RIP)

To define a neighboring router with which to exchange Routing Information Protocol (RIP) protocol information, use the **neighbor** command in the appropriate configuration mode. To remove an entry, use the **no** form of this command.

neighbor *ip-address*

no neighbor *ip-address*

Syntax Description	<i>ip-address</i>	IP address of a peer router with which routing information is exchanged.

Defaults	No neighboring routers are defined.

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **neighbor** command to permit the point-to-point (nonbroadcast) exchange of routing information. When it is used in combination with the **passive-interface** command in router configuration mode, routing information can be exchanged between a subset of routers and access servers on a LAN.

Multiple **neighbor** commands can be used to specify additional neighbors or peers.

Task ID	Task ID	Operations
	rip	read, write

Examples	The following example shows how to permit the sending of RIP updates to specific neighbors. One copy of the update is generated per neighbor:

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)# vrf vpn-1
RP/0/RP0/CPU0:router(config-rip-vrf)# neighbor 172.16.1.2
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	passive-interface (RIP)	Suppresses the sending of RIP updates on an interface.

R3.3 Beta Draft—Cisco Confidential Information

nsf (RIP)

To configure nonstop forwarding (NSF) on Routing Information Protocol (RIP) routes after a RIP process shutdown or restart, use the **nsf** command in the appropriate configuration mode. To remove this command from the configuration file and restore the system to its default condition, use the **no** form of this command.

nsf

no nsf

Syntax Description	This command has no arguments or keywords.

Defaults	NSF is disabled.

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	When you use the nsf command, NSF lifetime is automatically set to two times the update time (with a minimum value of 60 seconds). The RIP process must reconverge within this time. If the convergence exceeds the NSF lifetime, routes are purged from the Routing Information Base (RIB) and NSF may fail.

Task ID	Task ID	Operations
	rip	read, write

Examples	The following example shows how to configure RIP NSF:

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)# vrf vpn-1
RP/0/RP0/CPU0:router(config-rip-vrf)# nsf
```


R3.3 Beta Draft—Cisco Confidential Information

output-delay

To change the interpacket delay for Routing Information Protocol (RIP) updates send, use the **output-delay** command in the appropriate configuration mode. To remove the delay, use the **no** form of this command.

output-delay *delay*

no output-delay *delay*

Syntax Description	<i>delay</i>	Delay (in milliseconds) between packets in a multiple-packet RIP update. The range is from 8 to 50.

Defaults	The default is no delay.

Command Modes	Router configuration VRF configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the output-delay command if you are sending at high speed to a low-speed router that might not be able to receive at the high speed. Configuring this command helps prevent the routing table from losing information.

Task ID	Task ID	Operations
	rip	read, write

Examples	The following example shows how to set the interpacket delay to 10 milliseconds:

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)# vrf vpn-1
RP/0/RP0/CPU0:router(config-rip-vrf)# output-delay 10
```

R3.3 Beta Draft—Cisco Confidential Information

passive-interface (RIP)

To suppress the sending of Routing Information Protocol (RIP) updates on an interface, use the **passive-interface** command in interface configuration mode. To unsuppress updates, use the **no** form of this command.

passive-interface

no passive-interface

Syntax Description This command has no arguments or keywords.

Defaults RIP updates are sent on the interface.

Command Modes Interface configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

While RIP stops sending routing updates to the multicast (or broadcast) address on a passive interface, RIP continues to receive and process routing updates from its neighbors on that interface.

Task ID

Task ID	Operations
rip	read, write

Examples

The following example shows that Packet-over-SONET/SDH (POS) interface 0/1/0/0 stops multicasting (or broadcasting) RIP updates while continuing to receive RIP updates normally. POS interface 0/1/0/3 sends and receives updates normally. Also RIP updates are unicast to neighbor 172.168.1.2 over the appropriate interface:

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)# neighbor 172.16.1.2
RP/0/RP0/CPU0:router(config-rip)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-rip-if)# passive-interface
RP/0/RP0/CPU0:router(config-rip-if)# exit
RP/0/RP0/CPU0:router(config-rip)# interface pos 0/1/0/3
RP/0/RP0/CPU0:router(config-rip-if)# exit
```

R3.3 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	neighbor (RIP)	Defines a neighboring router with which to exchange RIP protocol information.

R3.3 Beta Draft—Cisco Confidential Information

poison-reverse disable

To disable poison reverse processing of Routing Information Protocol (RIP) router updates, use the **poison-reverse disable** command in interface configuration mode. To reenable poison reverse processing of RIP updates, use the **no** form of this command.

poison-reverse disable

no poison-reverse disable

Syntax Description This command has no arguments or keywords.

Defaults Poison reverse processing is enabled.

Command Modes Interface configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **poison-reverse disable** command to disable poison reverse processing of RIP router updates. The system default is that routes learned through RIP are advertised out the interface over which they were learned, but with an unreachable metric. If both poison reverse and split horizon are configured, then simple split horizon behavior (suppression of routes out of the interface over which they were learned) is replaced by poison reverse behavior. If split horizon is disabled, the poison reverse configuration is ignored.

Task ID

Task ID	Operations
rip	read, write

Examples

The following example shows how to disable poison reverse processing for a interface running RIP:

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-rip-if)# poison-reverse disable
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	split-horizon disable (RIP)	Disables the split horizon mechanism.

R3.3 Beta Draft—Cisco Confidential Information

receive version

To configure the Routing Information Protocol (RIP) interface to accept version-specific packets, use the **receive version** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

receive version {1 | 2 | 1 2}

no receive version {1 | 2 | 1 2}

Syntax Description

1	Version 1 packets.
2	Version 2 packets.
1 2	Both versions 1 and 2 packets.

Defaults

Version 2

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **receive version** command to override the default behavior of RIP. This command applies only to the interface being configured.

Task ID

Task ID	Operations
rip	read, write

Examples

The following example shows how to configure an interface to accept both RIP Version 1 and 2 packets:

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-rip-if)# receive version 1 2
```

Related Commands

Command	Description
send version	Configures the RIP interface to send version specific packets.

R3.3 Beta Draft—Cisco Confidential Information

redistribute (RIP)

To redistribute routes from one routing domain into Routing Information Protocol (RIP), use the **redistribute** command in the appropriate configuration mode. To remove the **redistribute** command from the configuration file and restore the system to its default condition in which the software does not redistribute routes, use the **no** form of this command.

Border Gateway Protocol (BGP)

redistribute bgp *process-id* [[**external** | **internal** | **local**] **route-policy** *name*]

no redistribute bgp *process-id*

Local Interface Routes

redistribute connected [**route-policy** *name*]

no redistribute connected

Enhanced Interior Gateway Routing Protocol (EIGRP)

redistribute eigrp *process-id* [**route-policy** *name*]

no redistribute eigrp *process-id*

Intermediate System-to-Intermediate System (ISIS)

redistribute isis *process-id* [**level-1** | **level-1-2** | **level-2**] [**route-policy** *name*]

no redistribute isis *process-id*

Open Shortest Path First (OSPF)

redistribute ospf *process-id* [**match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]] }
[**route-policy** *name*]

no redistribute ospf *process-id*

IP Static Routes

redistribute static [**route-policy** *name*]

no redistribute static

R3.3 Beta Draft—Cisco Confidential Information

Syntax Description		
	bgp	Distributes routes from the BGP protocol.
	<i>process-id</i>	For the bgp keyword, an autonomous system number, which is a 16 bit decimal number. Range is 1 to 65535. For the eigrp keyword, an EIGRP instance name from which routes are to be redistributed. The value takes the form of a string. A decimal number can be entered, but it is stored internally as a string. For the isis keyword, an IS-IS instance name from which routes are to be redistributed. The value takes the form of a string. A decimal number can be entered, but it is stored internally as a string. For the ospf keyword, an OSPF instance name from which routes are to be redistributed. The value takes the form of a string. A decimal number can be entered, but it is stored internally as a string.
	external	(Optional) Specifies BGP external routes only.
	internal	(Optional) Specifies BGP internal routes only.
	local	(Optional) Specifies BGP local routes only.
	route-policy <i>name</i>	(Optional) Specifies the identifier of a configured policy. A policy is used to filter the importation of routes from this source routing protocol to RIP.
	level-1	(Optional) Redistributes Level 1 IS-IS routes into other routing protocols independently.
	level-1-2	(Optional) Distributes both Level 1 and Level 2 IS-IS routes into other routing protocols.
	level-2	(Optional) Distributes Level 2 IS-IS routes into other routing protocols independently.
	[match { external [1 2] internal nssa-external [1 2] } [route-policy name]	(Optional) Specifies the criteria by which OSPF routes are redistributed into other routing domains. It can be one or more of the following: • internal—Routes that are internal to a specific autonomous system (intra- and inter-area OSPF routes). • external [1 2]—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 external routes. • nssa-external [1 2]—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 or Type 2 not-so-stubby area (NSSA) external routes. For the external and nssa-external options, if a type is not specified, then both Type 1 and Type 2 are assumed. If no match is specified, the default is no filtering.
	static	Redistributes IP static routes.

Defaults Route redistribution is disabled.

Command Modes Router configuration
VRF configuration

R3.3 Beta Draft—Cisco Confidential Information

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Redistributed routing information may be filtered by the **route-policy** *name* keyword and argument. This filtering ensures that only those routes intended by the administrator are redistributed by RIP.

For information about routing policies, see the *Routing Policy Commands on Cisco IOS XR Software* module of the *Cisco IOS XR Routing Command Reference*.

Task ID

Task ID	Operations
rip	read, write

Examples

The following example shows how to cause BGP routes to be redistributed into a RIP process:

```
RP/0/RP0/CPU0:router(config)# router rip  
RP/0/RP0/CPU0:router(config-rip)# redistribute bgp 100
```

Related Commands

Command	Description
default-metric (RIP)	Sets default metric values for routes redistributed from other protocols into RIP.

R3.3 Beta Draft – Cisco Confidential Information

router rip

To configure a routing process and enter router configuration mode for a Routing Information Protocol (RIP) process, use the **router rip** command in global configuration mode. To turn off the RIP routing process, use the **no** form of this command.

router rip

no router rip

Syntax Description This command has no arguments or keywords.

Defaults No router process is defined.

Command Modes Global

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	rip	read, write

Examples The following example shows how to configure a router process for RIP:

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)#
```

R3.3 Beta Draft – Cisco Confidential Information

route-policy (RIP)

To apply a routing policy to updates advertised to or received from a Routing Information Protocol (RIP) neighbor, use the **route-policy** command in the appropriate configuration mode. To disable applying routing policy to updates, use the **no** form of this command.

route-policy name {in | out}

no route-policy name {in | out}

Syntax Description

<i>name</i>	Name of route policy.
in	Applies policy to inbound routes.
out	Applies policy to outbound routes.

Defaults

No policy is applied.

Command Modes

Router configuration
VRF configuration
Interface configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **route-policy** command to specify a routing policy for an inbound or outbound route. The policy can be used to filter routes or modify route attributes.



Note

If a route policy is configured both on the interface and on the VRF, the interface route policy will be applied.

Task ID

Task ID	Operations
rip	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to filter routing updates received on an interface:

```
RP/0/RP0/CPU0:router(config)# router rip  
RP/0/RP0/CPU0:router(config-rip)# interface pos 0/1/0/0  
RP/0/RP0/CPU0:router(config-rip-if)# route-policy updpol-1 in
```

R3.3 Beta Draft—Cisco Confidential Information

send version

To configure the Routing Information Protocol (RIP) interface to send version specific packets, use the **send version** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

```
send version {1 | 2 | 1 2}
```

```
no send version {1 | 2 | 1 2}
```

Syntax Description	1	Version 1 packets.
	2	Version 2 packets.
	1 2	Both versions 1 and 2 packets.

Defaults	Version 2

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the send version command to override the default behavior of RIP. This command applies only to the interface being configured.

Task ID	Task ID	Operations
	rip	read, write

Examples	The following example shows how to configure an interface to send only RIP Version 2 packets:

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-rip-if)# send version 2
```

Related Commands	Command	Description
	receive version	Configures the RIP interface to accept version specific packets.

R3.3 Beta Draft—Cisco Confidential Information

show rip

To display all database and interface entry information from the Routing Information Protocol (RIP) topology table, use the **show rip** command in EXEC mode.

show rip [**vrf** {*vrf* | **all**}]

Syntax Description

vrf { <i>vrf</i> all }	(Optional) Specifies a particular VPN routing and forwarding (VRF) instance or all VRF instances.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
rip	read

Examples

The following example is sample output from the **show rip** command:

```
RP/0/RP0/CPU0:router# show rip
```

```
RIP config:
Active?:                               Yes
Out-of-memory state:                   Normal
Version:                               2
Default metric:                         Not set
Maximum paths:                         4
Auto summarize?:                       No
Broadcast for V2?:                     No
Packet source validation?:             Yes
Timers: Update:                        20 seconds (7 seconds until next update)
      Invalid:                          60 seconds
      Holddown:                         60 seconds
      Flush:                            65 seconds
```

R3.3 Beta Draft—Cisco Confidential Information**Table 130** *show rip Field Descriptions*

Field	Description
Active?	Active state setting.
Out-of-memory state	Out-of-memory state for RIP can be one of the following: Normal, Minor, Severe, or Critical.
Version	Version number is 2.
Default metric	Default metric value, if configured. Otherwise Not set.
Maximum paths	Number of maximum paths allowed per RIP route.
Auto summarize?	Auto-summarize state setting.
Broadcast for V2?	RIP Version 2 broadcast setting.
Packet source validation?	Validation setting for the source IP address of incoming routing updates to RIP.
Timers	RIP network timer settings.

R3.3 Beta Draft—Cisco Confidential Information

show rip database

To display database entry information from the Routing Information Protocol (RIP) topology table, use the **show rip database** command in EXEC mode.

show rip [**vrf** {*vrf* | **all**}] **database** [*prefix/length* | *ip-address mask*]

Syntax Description

vrf { <i>vrf</i> all }	(Optional) Specifies a particular VPN routing and forwarding (VRF) instance or all VRF instances.
<i>prefix-length</i>	(Optional) The <i>prefix-length</i> argument specifies the length of the IP prefix. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash between must precede the decimal value. Range is 0 to 32 for IPv4 addresses.
<i>ip-address</i>	(Optional) Network IP address about which routing information should be displayed.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Summary address entries appear in the database only if relevant child routes are summarized. When the last child route for a summary address becomes invalid, the summary address is also removed from the routing table.

Task ID

Task ID	Operations
rip	read

Examples

The following is sample output from the **show rip database** command:

```
RP/0/RP0/CPU0:router# show rip database
```

```
Routes held in RIP's topology database:
 10.0.0.0/24
```


R3.3 Beta Draft—Cisco Confidential Information

```
[0]      directly connected, GigabitEthernet0/6/0/0
10.0.0.0/8      auto-summary
12.0.0.0/24
[5] distance: 20      redistributed
12.0.0.0/8      auto-summary
50.50.0.0/24
[1] via 10.0.0.20, next hop 10.0.0.20, Uptime: 1s, GigabitEthernet0/6/0/0
50.50.1.0/24 (inactive)
[1] via 10.0.0.20, next hop 10.0.0.20, Uptime: 1s, GigabitEthernet0/6/0/0
50.0.0.0/8      auto-summary
90.90.0.0/24
[5] distance: 20      redistributed
90.90.1.0/24
[5] distance: 20      redistributed
```

R3.3 Beta Draft—Cisco Confidential Information

show rip interface

To display interface entry information from the Routing Information Protocol (RIP) topology table, use the **show rip interface** command in EXEC mode.

show rip [**vrf** {*vrf* | **all**}] **interface** *type instance*

Syntax Description

vrf { <i>vrf</i> all }	(Optional) Specifies a particular VPN routing and forwarding (VRF) instance or all VRF instances.
<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>instance</i>	Either a physical interface instance or a virtual interface instance: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID

Task ID	Operations
rip	read

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example is sample output from the **show rip interface** command:

```
RP/0/RP0/CPU0:router# show rip interface

GigabitEthernet0_6_0_0
Rip enabled?:                Yes
Out-of-memory state:         Normal
Broadcast for V2:             No
Accept Metric 0?:            No
Send versions:                0
Receive versions:             0
Interface state:              Up
IP address:                   10.0.0.12/24
Metric Cost:                  0
Split horizon:                Enabled
Poison Reverse:               Enabled

GigabitEthernet0_6_0_2
Out-of-memory state:         Normal
Rip enabled?:                Yes
Broadcast for V2:             No
Accept Metric 0?:            No
Send versions:                0
Receive versions:             0
Interface state:              Up
IP address:                   12.0.0.12/24
Metric Cost:                  0
Split horizon:                Enabled
Poison Reverse:               Enabled
RIP peers attached to this interface:
  12.0.0.13
    uptime: 3      version: 2
    packets discarded: 0    routes discarded: 402
```

R3.3 Beta Draft—Cisco Confidential Information

show rip statistics

To display statistical entry information from the Routing Information Protocol (RIP) topology table, use the **show rip statistics** command in EXEC mode.

show rip [vrf {vrf | all}] statistics

Syntax Description	vrf {vrf all}	(Optional) Specifies a particular VPN routing and forwarding (VRF) instance or all VRF instances.

Defaults	No default behavior or values

Command Modes	EXEC

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	rip	read

Examples	The following example is sample output from the show rip statistics command:

```
RP/0/RP0/CPU0:router# show rip statistics
```

```
RIP statistics:
  Total messages sent:      5597
  Message send failures:    0
  Regular updates sent:    5566
  Queries responded to:    0
  RIB updates:             6
  Total packets received:  5743
  Discarded packets:       0
  Discarded routes:        0
  Number of routes allocated: 18
  Number of paths allocated: 14
  Route malloc failures:    0
  Path malloc failures:     0
```

R3.3 Beta Draft—Cisco Confidential Information

site-of-origin

To configure the Site of Origin (SoO) filtering on a Routing Information Protocol (RIP) interface, use the **site-of-origin** command in interface configuration mode. To disable SoO filtering on an interface, use the **no** form of this command.

site-of-origin {*as-number:number* | *ip-address:number*}

no site-of-origin {*as-number:number* | *ip-address:number*}

Syntax Description

<i>as-number:</i>	Autonomous system number. Range is from 1 to 65535. The colon is used to separate the autonomous system number and network number.
<i>number</i>	Network number. Range is from 1 to 4294967295.
<i>ip-address:</i>	The IP address argument specifies the IP address in four-part, dotted-decimal notation. The colon is used to separate the IP address and network number.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

A RIP process must be capable of retrieving the SoO attribute on routes redistributed from the Border Gateway Protocol (BGP) when required to support complex topologies that include MPLS VPN links between sites with back-door links.

Use the **site-of-origin** command to set an SoO BGP extended community attribute that is used to identify routes that have originated from a site so that the re-advertisement of that prefix back to the source site can be prevented. The SoO extended community uniquely identifies the site from which a Provider Edge (PE) router has learned a route.

Task ID

Task ID	Operations
rip	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to configure SoO filtering on a RIP interface:

```
RP/0/RP0/CPU0:router(config)# router rip  
RP/0/RP0/CPU0:router(config-rip) interface pos 0/1/0/0  
RP/0/RP0/CPU0:router(config-rip-if)# site-of-origin 10.0.0.1:20
```

R3.3 Beta Draft—Cisco Confidential Information

split-horizon disable (RIP)

To disable split horizon for a Routing Information Protocol (RIP) process, use the **split-horizon disable** command in interface configuration mode. To enable split horizon, use the **no** form of this command.

split-horizon disable

no split-horizon disable

Syntax Description This command has no arguments or keywords.

Defaults Split horizon is enabled for a RIP process.

Command Modes Interface configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

As an alternative, you can explicitly specify the **split-horizon disable** command in your configuration. However, if you do so, you must similarly disable split horizon for all routers and access servers in any relevant multicast groups on that network.

If split horizon is disabled, the poison reverse configuration is ignored.



Note

In general, we recommend that you do not change the default state of split horizon unless you are certain that your application requires the change to properly advertise routes.

Task ID	Task ID	Operations
	rip	read, write

Examples The following example shows how to disable split horizon on a Packet-over-Sonet/SDH link:

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)# interface pos 0/1/0/0
RP/0/RP0/CPU0:router(config-rip-if)# split-horizon disable
```

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	poison-reverse disable	Disables poison reverse processing of RIP router updates.

R3.3 Beta Draft—Cisco Confidential Information

timers basic

To adjust Routing Information Protocol (RIP) network timers, use the **timers basic** command in router configuration mode. To restore the default timers, use the **no** form of this command.

timers basic *update invalid holddown flush*

no timers basic

Syntax Description		
<i>update</i>		Rate, in seconds, at which updates are sent. This is the fundamental timing parameter of the routing protocol.
<i>invalid</i>		Interval, in seconds, after which a route is declared invalid; it should be at least three times the value of the update argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters into a holddown state. The route is marked inaccessible and is advertised as unreachable.
<i>holddown</i>		Interval, in seconds, during which routing information regarding better paths is suppressed. It should be at least three times the value of the update argument. A route enters into a holddown state when an update packet is received that indicates that the route is unreachable. The route is marked inaccessible and is advertised as unreachable. When holddown expires, routes advertised by other sources are accepted, and the route is no longer inaccessible.
<i>flush</i>		Amount of time, in seconds, that must pass before the route is removed from the routing table; the interval specified should be greater than the value of the <i>invalid</i> argument. If it is less than invalid timer value, the proper holddown interval cannot elapse, which results in a new route being accepted before the holddown interval expires.

Defaults

update: 30 seconds
invalid: 180 seconds
holddown: 180 seconds
flush: 240 seconds

Command Modes

Router configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft – Cisco Confidential Information

The basic timing parameters for RIP are adjustable. Because RIP is running a distributed, asynchronous routing algorithm, these timers must be the same for all routers in the network.



Note

The current and default timer values may be viewed by using the **show rip** command.

Task ID

Task ID	Operations
rip	read, write

Examples

The following example shows how to set updates to be broadcast every 5 seconds. If a router is not heard from in 15 seconds, the route is declared unusable. Further information is suppressed for an additional 15 seconds. At the end of the flush period, the route is flushed from the routing table.

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip) timers basic 5 15 15 30
```

Related Commands

Command	Description
show rip	Displays all database and interface entry information from the RIP topology table.

R3.3 Beta Draft—Cisco Confidential Information

validate-update-source disable

To stop the Cisco IOS XR software from validating the source IP address of incoming routing updates for Routing Information Protocol (RIP), use the **validate-update-source disable** command in router configuration mode. To reenable this function, use the **no** form of this command.

validate-update-source disable

no validate-update-source disable

Syntax Description	This command has no arguments or keywords.

Defaults	The source IP address of incoming updates for RIP is always validated.

Command Modes	Interface configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

When the **validate-update-source disable** command is used, validation is not performed.

By default, the software ensures that the source IP address of incoming routing updates is on the same IP network as one of the addresses defined for the receiving interface.

Disabling split horizon on the incoming interface also causes the system to perform this validation check.

For unnumbered IP interfaces (interfaces configured as IP unnumbered), no checking is performed.

Task ID	Task ID	Operations
	rip	read, write

Examples	The following example shows how to disable split horizon on a Packet-over-Sonet link:

```
RP/0/RP0/CPU0:router(config)# router rip
```

```
RP/0/RP0/CPU0:router(config-rip) validate-update-source disable
```

R3.3 Beta Draft—Cisco Confidential Information**vrf (RIP)**

To define a VPN routing and forwarding (VRF) instance and to enter VRF configuration mode, use the **vrf** command in router configuration mode. To remove a VRF instance use the no form of this command.

vrf *vrf-name*

no vrf *vrf-name*

Syntax Description	<i>vrf-name</i> Specifies a particular VPN routing and forwarding instance.					
Defaults	No VRFs are defined. No import or export lists are associated with a VRF. No route maps are associated with a VRF.					
Command Modes	Router configuration					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>Release 3.3</td><td>This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.</td></tr></table>		Release	Modification	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.
Release	Modification					
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.					
Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the vrf command to configure a VRF instance. A VRF instance is a collection of VPN routing and forwarding tables maintained at the provider edge (PE) router. From VRF configuration mode, you can issue all commands available in router configuration mode such as the auto-summary command.					
Task ID	<table><tr><th>Task ID</th><th>Operations</th></tr><tr><td>rip</td><td>read, write</td></tr></table>		Task ID	Operations	rip	read, write
Task ID	Operations					
rip	read, write					

Examples

The following example shows how to enter VRF configuration mode and identify RIP commands that can be issued from that mode.

```
RP/0/RP0/CPU0:router(config)# router rip
RP/0/RP0/CPU0:router(config-rip)# vrf vpn-1
RP/0/RP0/CPU0:router(config-rip-vrf)# ?
```

auto-summary	Enable automatic network number summarization
broadcast-for-v2	Send RIP v2 output packets to broadcast address
commit	Commit the configuration changes to running
default-information	Control distribution of default information

R3.3 Beta Draft—Cisco Confidential Information

default-metric	Set metric of redistributed routes
describe	Describe a command without taking real actions
distance	Define an administrative distance
do	Run an exec command
exit	Exit from this submode
interface	Enter the RIP interface configuration submode
maximum-paths	Maximum number of paths allowed per route
neighbor	Specify a neighbor router
no	Negate a command or set its defaults
nsf	Enable Cisco Non Stop Forwarding
output-delay	Interpacket delay for RIP updates
redistribute	Redistribute information from another routing protocol
route-policy	Apply route policy to routing updates
show	Show contents of configuration
timers	Adjust routing timers
validate-update-source	Validate source address of routing updates

RP/0/RP0/CPU0:router(config-rip-vrf)#

R3.3 Beta Draft – Cisco Confidential Information

Routing Policy Language Commands on Cisco IOS XR Software

Beta Draft Cisco Confidential Information

This chapter describes the Cisco IOS XR software routing policy language (RPL) commands used to create, modify, monitor, and maintain routing policies.

For detailed information about RPL concepts, configuration tasks, and examples, see the *Implementing Routing Policy on Cisco IOS XR Software* configuration guide.

R3.3 Beta Draft – Cisco Confidential Information

abort

To discard a route policy definition and return to global configuration mode, use the **abort** command in route-policy configuration mode.

abort

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or value

Command Modes	Route-policy configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	route-policy	read, write

Examples	The following example shows how to discard a route policy that was started and return to global configuration mode:

```
RP/0/RP0/CPU0:router(config)# route-policy policy_1
RP/0/RP0/CPU0:router(config-rpl)# if as-path is-local then
RP/0/RP0/CPU0:router(config-rpl-if)# abort
RP/0/RP0/CPU0:router(config)#
```


R3.3 Beta Draft – Cisco Confidential Information

add

To add an offset to an existing value, use the **add** command in route-policy configuration mode.

add { **eigrp-metric** *bandwidth* | **rip-metric** { *number* | *parameter* }

Syntax Description	eigrp-metric	Enhanced Interior Gateway Routing Protocol (EIGRP), metric attribute.
	<i>bandwidth</i>	Bandwidth in kilobits per second. Range is from 0 to 4294967295.
	rip-metric	Routing Information Protocol (RIP) metric attribute.
	<i>number</i>	Four bit decimal number. Range is from 0 to 16.
	<i>parameter</i>	Parameter name. The parameter name must be preceded with a "\$."

Defaults No default behavior or value

Command Modes Route-policy configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Task ID	Task ID	Operations
	route-policy	read, write

Examples The following example shows how to add 1000 kilobits per second to the EIGRP metric:

```
RP/0/RP0/CPU0:router(config)# route-policy policy_1
RP/0/RP0/CPU0:router(config-rpl)# add eigrp-metric 1000
RP/0/RP0/CPU0:router(config-rpl)# end-policy
```

R3.3 Beta Draft—Cisco Confidential Information

apply

To execute a parameterized or unparameterized policy from within another policy, use the **apply** command in route-policy configuration mode.

apply *name* [*parameter1*, *parameter2*, . . . , *parameterN*]

Syntax Description

<i>name</i>	Name of a route policy.
<i>parameter</i>	(Optional) Parameter value to be passed to the applied route policy.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **apply** command to execute a policy (either parameterized or unparameterized) from within another policy, which allows for the reuse of common blocks of policy.

Task ID

Task ID	Operations
route-policy	read, write

Examples

In the following example, the policy CustomerIn applies the route-policy SetLocalPref to conditionally set the local preference on a route. The parameters 20, 30, 40, and 50 are passed to the parameterized policy SetLocalPref, where the local preference is set to:

- 20, if the community 217:20 is present in the route
- 30, if the community 217:30 is present in the route
- 40, if the community 217:40 is present in the route
- 50, if the community 217:50 is present in the route

R3.3 Beta Draft—Cisco Confidential Information

```
RP/0/RP0/CPU0:router(config)# route-policy CustomerIn
RP/0/RP0/CPU0:router(config-rpl)# apply SetLocalPref (20, 30, 40, 50)
RP/0/RP0/CPU0:router(config-rpl)# end-policy

RP/0/RP0/CPU0:router(config)# route-policy SetLocalPref ($lp1, $lp2, $lp3, $lp4)
RP/0/RP0/CPU0:router(config-rpl)# if community matches-any (217:$lp1) then
RP/0/RP0/CPU0:router(config-rpl-if)# set local-preference $lp1
RP/0/RP0/CPU0:router(config-rpl-if)# elseif community matches-any (217:$lp2) then
RP/0/RP0/CPU0:router(config-rpl-if)# set local-preference $lp2
RP/0/RP0/CPU0:router(config-rpl-if)# elseif community matches-any (217:$lp3) then
RP/0/RP0/CPU0:router(config-rpl-if)# set local-preference $lp3
RP/0/RP0/CPU0:router(config-rpl-if)# elseif community matches-any (217:$lp4) then
RP/0/RP0/CPU0:router(config-rpl-if)# set local-preference $lp4
RP/0/RP0/CPU0:router(config-rpl-if)# endif
RP/0/RP0/CPU0:router(config-rpl-if)# end-policy
```

R3.3 Beta Draft—Cisco Confidential Information

as-path in

To match the AS path of a route to an AS path set, use the **as-path in** command in route-policy configuration mode.

as-path in {*as-path-set-name* | *inline-as-path-set*}

Syntax Description

<i>as-path-set-name</i>	Name of an AS path set.
<i>inline-as-path-set</i>	Name of an inline AS path set.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **as-path in** command as a conditional expression within an **if** statement to match the AS path of a route to an AS path set. The AS path is a sequence of autonomous system numbers traversed by a route.

**Note**

For a list of all conditional expressions available within an **if** statement, see the **if** command.

The **as-path in** command evaluates to true if at least one of the regular expressions defined in the associated AS path set matches the AS path attribute of the route.

In the case where the AS path set is defined but contains no elements in it, the **as-path in** conditional expression command returns false.

Task ID

Task ID	Operations
route-policy	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

For example, assume we have an AS path set named my-as-set defined as follows:

```
RP/0/RP0/CPU0:router(config)# as-path-set my-as-set  
RP/0/RP0/CPU0:router(config-as)# ios-regex '_12$',  
RP/0/RP0/CPU0:router(config-as)# ios-regex '_13$'  
RP/0/RP0/CPU0:router(config-as)# end-set
```

and the following policy excerpt using an *as-path-set-name* argument:

```
RP/0/RP0/CPU0:router(config-rpl)# if as-path in my-as-set then  
RP/0/RP0/CPU0:router(config-rpl)# set local-preference 100  
RP/0/RP0/CPU0:router(config-rpl)# endif
```

The AS path in condition evaluates to true if one or more of the regular expression matches in the set my-as-set match the AS path associated with the route. In the case of a defined but empty AS path set, this operator returns false.

The preceding policy excerpt is equivalent to the following version, which uses an *inline-as-path-set*:

```
RP/0/RP0/CPU0:router(config-rpl)# if as-path in (ios-regex '_12$',ios-regex '_13$') then  
RP/0/RP0/CPU0:router(config-rpl-if)# set local-preference 100  
RP/0/RP0/CPU0:router(config-rpl-if)# endif
```

R3.3 Beta Draft—Cisco Confidential Information

as-path is-local

To determine if this router or another router within this autonomous system or confederation originated a route, use the **as-path is-local** command in route-policy configuration mode.

as-path is-local

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or value

Command Modes Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **as-path is-local** command as a conditional expression within an **if** statement to determine if this router (or another router within this autonomous system or confederation) originated the route.



Note For a list of all conditional expressions available within an **if** statement, see the **if** command.

Routes that are locally originated within the autonomous system or confederation carry an empty AS path. For the Border Gateway Protocol (BGP) specification, when a route is advertised across the autonomous system boundary or a confederation boundary, the local autonomous system number or confederation ID is appended to the autonomous system path. The AS path of a locally originated aggregate is also empty unless it has been modified by policy.

The **is-local** operator evaluates to true for autonomous system paths that are empty. An empty AS path is how an AS path that is local to our autonomous system is represented in BGP.

Task ID	Task ID	Operations
	route-policy	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

In the following example, if the AS path is local, then the local preference is set to 100:

```
RP/0/RP0/CPU0:router(config-rpl)# if as-path is-local then  
RP/0/RP0/CPU0:router(config-rpl-if)# set local-preference 100  
RP/0/RP0/CPU0:router(config-rpl-if)# endif
```

R3.3 Beta Draft—Cisco Confidential Information

as-path length

To perform conditional checks based on the length of the AS path, use the **as-path length** command in route-policy configuration mode.

as-path length {**eq** | **is** | **ge** | **le**} {*integer* | *parameter*}

Syntax Description

eq is ge le	Equal to; greater than or equal to; less than or equal to.
<i>integer</i>	Length of the AS path as an integer value.
<i>parameter</i>	Length of the AS path as a parameter value.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **as-path length** command as a conditional expression within an **if** statement to perform a conditional check based on the length of the AS path.

**Note**

For a list of all conditional expressions available within an **if** statement, see the **if** command.

This command takes either a specific integer value or a range of integer values specified with the **ge** and **le** operators. Any or all of these integers can be parameterized. The operator counts one for each autonomous system in the path. In the case where the route may be aggregated and contain one or more as-sets, the length operator adds one for each set present, the occurrence of an as-set typically indicates that this route is an aggregated route, and the aggregated route had a component route that contained one of the autonomous systems in the set. Likewise, in the case of confederations, a count of one is added for each confederation in the path or each confederation set in the path. A null AS path has a length of zero.

Task ID

Task ID	Operations
route-policy	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

In the following example, if the AS path length equals 10, then the local preference is set to 100:

```
RP/0/RP0/CPU0:router(config-rpl)# if as-path length eq 10 then
RP/0/RP0/CPU0:router(config-rpl-if)# set local-preference 100
RP/0/RP0/CPU0:router(config-rpl-if)# endif
```

Related Commands

Command	Description
as-path in	Matches the AS path of a route to an AS path set.
as-path originates-from	Compares an AS path to the autonomous system sequence beginning with the autonomous system number that originated a route.
as-path passes-through	Tests to learn if the supplied integer or parameter appears anywhere in the AS path.
as-path unique-length	Performs specific checks based on the length of the AS path.

R3.3 Beta Draft—Cisco Confidential Information

as-path neighbor-is

To test to learn if the sequence of autonomous system numbers matches the path beginning with the neighboring autonomous system from which a route was heard, use the **as-path neighbor-is** command in route-policy configuration mode.

as-path neighbor-is *as-number-list* [**exact**]

Syntax Description

<i>as-number-list</i>	Numbers or parameters, enclosed in single quotation marks, that represent a sequence of autonomous system numbers. Range is 0 to 65535.
exact	(Optional) Specifies that with the exact keyword, the <i>as-number-list</i> value must identically match the AS path for the route; without the exact keyword, any element in the <i>as-number-list</i> argument matches one or more occurrences of that element in the AS path for the route.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **as-path neighbor-is** command as a conditional expression within an **if** statement to test the autonomous system number or numbers at the head of the AS path against a sequence of one or more integral values or parameters, in other words, to test to learn if the sequence of autonomous system numbers matches the path beginning with the neighboring autonomous system from which this route was heard.

**Note**

For a list of all conditional expressions available within an **if** statement, see the **if** command.

This command has an equivalent regular expression (ios-regex). For example, AS path neighbor-is '1' would be '^1_'.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	route-policy	read, write

Examples

The following are incomplete configuration examples:

```
RP/0/RP0/CPU0:router(config-rpl)# if as-path neighbor-is '10' then
RP/0/RP0/CPU0:router(config-rpl)# if as-path neighbor-is '$asnum' then
RP/0/RP0/CPU0:router(config-rpl)# if as-path neighbor-is '10 20' then
```

These statements evaluate to true when the first autonomous system numbers on the AS path match, in the same order, the supplied parameters or integer values in the **neighbor-is** statement. If the neighboring autonomous system location happens to be an AS-set, the operator evaluates to true if the corresponding argument to the **neighbor-is** operator is an element of the AS-set.

Without the **exact** keyword, repeated autonomous system numbers in the AS path are ignored. For example,

```
RP/0/RP0/CPU0:router(config-rpl)# if as-path neighbor-is '10 20' then
```

matches an AS path beginning

```
10 10 10 20 ...
```

and an AS path beginning:

```
10 20 ....
```

With the **exact** keyword, repetitions are not ignored, therefore

```
RP/0/RP0/CPU0:router(config-rpl)# if as-path neighbor-is '10 20' exact then
```

matches the second of these AS paths but not the first.

Related Commands	Command	Description
	as-path in	Matches the AS path of a route to an AS path set.
	as-path length	Performs conditional checks based on the length of the AS path.
	as-path originates-from	Compares an AS path to the autonomous system sequence beginning with the autonomous system number that originated a route.
	as-path passes-through	Tests to learn if the supplied integer or parameter appears anywhere in the AS path.
	as-path unique-length	Performs specific checks based on the length of the AS path.

R3.3 Beta Draft—Cisco Confidential Information

as-path originates-from

To compare an AS path against the autonomous system sequence beginning with the autonomous system number that originated a route, use the **as-path originates-from** command in route-policy configuration mode.

as-path originates-from *as-number-list* [**exact**]

Syntax Description

<i>as-number-list</i>	Numbers or parameters, enclosed in single quotation marks, that represent a sequence of autonomous system numbers. Range is 0 to 65535.
exact	(Optional) Specifies that without the exact keyword, repeated autonomous system numbers in the AS path are ignored; without the exact keyword, repetitions are not ignored.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **as-path originates-from** command as a conditional expression within an **if** statement to compare an AS path to the autonomous system sequence.

**Note**

For a list of all conditional expressions available within an **if** statement, see the **if** command.

The **originates-from** operator is similar to the **neighbor-is** operator, except that it looks at the autonomous system number at the opposite end of the AS path. In other words, it is comparing to the autonomous system that originated the route. It can take numbers or parameters, enclosed in single quotation marks, that represent a sequence of autonomous system numbers. When more than one number is specified in the list, the sequence of autonomous system numbers listed must appear as a subsequence in the AS path, with the last number corresponding to the autonomous system that originated the route.

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	route-policy	read, write

Examples

The following are incomplete configuration examples:

```
RP/0/RP0/CPU0:router(config-rpl)# if as-path originates-from '10 11' then
RP/0/RP0/CPU0:router(config-rpl)# if as-path originates-from '$asnum 11' then
```

The first line of the preceding example evaluates to true if autonomous system 11 originated the route and then advertised it to autonomous system 10, from which the route was eventually propagated to us. In the case where the route has been aggregated, and the location of the originating autonomous system contains an AS-set, the **originates-from** operator evaluates to true if the argument to the **originates-from** operator is contained in the AS-set.

Without the **exact** keyword, repeated autonomous system numbers in the AS path are ignored. For example,

```
RP/0/RP0/CPU0:router(config-rpl)# if as-path originates-from '10 11' then
```

matches an autonomous system path ending

```
...10 10 10 11
```

and an autonomous system path ending

```
...10 11
```

With the **exact** keyword, repetitions are not ignored, therefore

```
RP/0/RP0/CPU0:router(config-rpl)# if as-path originates-from '10 11' exact then
```

matches the second of these autonomous system paths but not the first.

Related Commands	Command	Description
	as-path in	Matches the AS path of a route to an AS path set.
	as-path length	Performs conditional checks based on the length of the AS path.
	as-path passes-through	Tests to learn if the supplied integer or parameter appears anywhere in the AS path.
	as-path unique-length	Performs specific checks based on the length of the AS path.

R3.3 Beta Draft—Cisco Confidential Information

as-path passes-through

To verify if the supplied integer or parameter appears anywhere in the AS path or if the supplied sequence of integers and parameters appears, in the same order, anywhere in the AS path, use the **as-path passes-through** command in route-policy configuration mode.

as-path passes-through *as-number-list* [**exact**]

Syntax Description

<i>as-number-list</i>	Numbers or parameters, enclosed in single quotation marks, that represent a sequence of autonomous system numbers. Range is 0 to 65535.
exact	(Optional) Specifies that without the exact keyword, repeated autonomous system numbers in the AS path are ignored; without the exact keyword, repetitions are not ignored.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **as-path passes-through** command as a conditional expression within an **if** statement to verify if the specified integer or parameter appears anywhere in the AS path or if the sequence of integers and parameters appears.

**Note**

For a list of all conditional expressions available within an **if** statement, see the **if** command.

The **passes-through** operator takes a sequence of integers or parameters, enclosed in single quotation marks, as an argument. It can also take a single integer or parameter as an argument. It evaluates to true if the supplied integer or parameter appears anywhere in the AS path, or if the supplied sequence of integers and parameters appears, in the same order, anywhere in the AS path. This includes the **originates-from** or **neighbor-is** location in the AS path.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	route-policy	read, write

Examples

The following are incomplete configuration examples:

```
RP/0/RP0/CPU0:router(config-rpl)# if as-path passes-through '10' then
RP/0/RP0/CPU0:router(config-rpl)# if as-path passes-through '$asnum' then
RP/0/RP0/CPU0:router(config-rpl)# if as-path passes-through '10 11' then
RP/0/RP0/CPU0:router(config-rpl)# if as-path passes-through '10 $asnum 12' then
```

Without the **exact** keyword, repeated autonomous system numbers in the AS path are ignored. For example:

```
RP/0/RP0/CPU0:router(config-rpl)# if as-path passes-through '9 10 11' then
```

matches an AS path containing

```
...9 10 10 10 11 ....
```

and an AS path containing:

```
...9 10 11...
```

With the **exact** keyword, repetitions are not ignored. Therefore:

```
RP/0/RP0/CPU0:router(config-rpl)# if as-path passes-through '9 10 11' exact then
```

matches the second of these AS paths but not the first.

Related Commands	Command	Description
	as-path in	Matches the AS path of a route to an AS path set.
	as-path length	Performs conditional checks based on the length of the AS path.
	as-path originates-from	Compares an AS path to the autonomous system sequence beginning with the autonomous system number that originated a route.
	as-path unique-length	Performs specific checks based on the length of the AS path.

R3.3 Beta Draft—Cisco Confidential Information

as-path-set

To create a named AS path set, use the **as-path-set** command in global configuration mode. To remove the named AS path set, use the **no** form of this command.

as-path-set *name*

no as-path-set *name*

Syntax Description

<i>name</i>	Name of the AS path set.

Defaults

No default behavior or value

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **as-path-set** command to create a named AS path set.

An AS path set comprises operations for matching an AS path attribute.

This command enters AS path set configuration mode, in which you can use the **ios-regex** keyword to indicate the type of regular expression. Single quotation marks are required around the regular expression.

The inline set form is a parenthesized list of comma-separated expressions.

See the “Understanding Regular Expressions, Special Characters and Patterns” appendix in the *Cisco IOS XR Getting Started Guide* for information about forming regular expressions.

Task ID

Task ID	Operations
route-policy	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following is a sample definition of an AS path set named aset1:

```
RP/0/RP0/CPU0:router(config)# as-path-set aset1  
RP/0/RP0/CPU0:router(config-as)# ios-regex '_42$',  
RP/0/RP0/CPU0:router(config-as)# ios-regex '_127$'  
RP/0/RP0/CPU0:router(config-as)# end-set
```

This AS path set is composed of two elements. When used in a matching operation, this AS path set matches any route whose AS path ends with either the autonomous system number 42 or 127.

The following is a sample of an inline set:

```
RP/0/RP0/CPU0:router(config-rpl)# if as-path in (ios-regex '_42$', ios-regex$ '_127$')  
RP/0/RP0/CPU0:router(config-rpl)# pass  
RP/0/RP0/CPU0:router(config-rpl)# endif
```

R3.3 Beta Draft—Cisco Confidential Information

as-path unique-length

To perform specific checks based on the length of the AS path, use the **as-path unique-length** command in route-policy configuration mode.

as-path unique-length {eq | is | ge | le} {integer | parameter}

Syntax Description

eq is ge le	Equal to; greater than or equal to; less than or equal to.
<i>integer</i>	Length of the AS path as an integer value.
<i>parameter</i>	Length of the AS path as a parameter value.

Defaults

No default behavior or values

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **as-path unique-length** command as a conditional expression within an **if** statement to perform a check based on the length of the AS path.

**Note**

For a list of all conditional expressions available within an **if** statement, see the **if** command.

The **unique-length** operator is similar to the **length** operator, except that when an AS path has been padded with the same autonomous system number multiple times, the operator counts only one when the route is padded. Therefore, given an AS path of 333 333 111 222 123 444 444 444, the **unique-length** operator would return a value of 5, whereas the **length** operator would return a value of 8.

Task ID

Task ID	Operations
route-policy	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to perform checks based on the AS path length. If the AS path matches the specified values, the local preference is set to 100:

```
RP/0/RP0/CPU0:router(config-rpl)# if as-path unique-length eq 10 then
RP/0/RP0/CPU0:router(config-rpl)# if as-path unique-length ge 10 then
RP/0/RP0/CPU0:router(config-rpl)# if as-path unique-length le 10 then

RP/0/RP0/CPU0:router(config-rpl)# if as-path unique-length eq $integerparam then
RP/0/RP0/CPU0:router(config-rpl)# if as-path unique-length ge $geparam then
RP/0/RP0/CPU0:router(config-rpl)# if as-path unique-length le $leparam then

RP/0/RP0/CPU0:router(config-rpl)# set local-preference 100
RP/0/RP0/CPU0:router(config-rpl)# endif
```

Related Commands

Command	Description
as-path length	Performs conditional checks based on the length of the AS path.

R3.3 Beta Draft—Cisco Confidential Information

community is-empty

To learn if a route has no community attributes associated with it, use the **community is-empty** command in route-policy configuration mode.

community is-empty

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **community is-empty** command as a conditional expression within an **if** statement to learn if a route has community attributes associated with it.



Note For a list of all conditional expressions available within an **if** statement, see the **if** command.

This command takes no arguments, and evaluates to true only if the route has no community attributes associated with it.

Task ID	Task ID	Operations
	route-policy	read, write

Examples In the following example, if the route has no community attributes associated with it, then the local preference is set to 100:

```
RP/0/RP0/CPU0:router(config-rpl)# if community is-empty then
RP/0/RP0/CPU0:router(config-rpl)# set local-preference 100
RP/0/RP0/CPU0:router(config-rpl)# endif
```

R3.3 Beta Draft—Cisco Confidential Information

community matches-any

To match any elements of a community set, use the **community matches-any** command in route-policy configuration mode.

community matches-any { *community-set-name* | *inline-community-set* }

Syntax Description

<i>community-set-name</i>	Name of a community set.
<i>inline-community-set</i>	Inline community set.

Defaults

No default behavior or values

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The BGP community matching operators were enhanced to allow comparisons on ranges and regular expressions.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **community matches-any** command as a conditional expression within an **if** statement to match any element of a community set.



Note

For a list of all conditional expressions available within an **if** statement, see the **if** command.

A simple condition using the **matches-any** operator evaluates as true if at least one community element of the community attribute for the route matches an element in the community set operand. If no community in the route matches any of the specifications in the named or inline set, then the condition evaluates to false. Likewise, when there is no community at all in the route, the condition evaluates to false.

Matching of a community in the route to a specification in a named or an inline set is intuitive. If the community specification in a set is the familiar colon-separated decimal 16-bit numbers specification, or one of the well-known communities, the community matches the specification if the specification denotes the same 32-bit number as that in the route. If the community specification uses a wildcard, then

R3.3 Beta Draft—Cisco Confidential Information

the community in the route matches if it is one of the many communities denoted by the wildcard specification. In inline sets, community specifications may be parameterized, in which case the relevant matching is done when the value of the parameter has been supplied.

Communities may also be matched using range and regular expression operators. Range specifications are entered as follows: *[low-value..high-value]*. Either or both colon-separated halves of a community value may contain a range. The following are valid range specifications:

```
10:[100..1000]
[10..100]:80
[10..100]:[100..2000]
```

In addition, the **private-as** keyword may be used to specify the range from 64512 to 65534. Regular expressions are specified as the **ios-regex** keyword followed by a valid regular expression string.

Community values from the route are matched one at a time to the match specifications. Therefore, regex match specifications are expected to represent one individual community value and not a sequence of community values.

Task ID	Task ID	Operations
	route-policy	read, write

Examples

In the following example, a named community set called my-community-set and a route policy called community-matches-any-example are created. The policy sets the local-preference to 100 for any route that has one or more of the communities in the my-community-set community set. If the route does not have any of these communities, the policy checks whether it has any communities whose first half is in the range from 10 to 25 and whose second half is the value 35, in which case it sets the local-preference to 200. Otherwise, it checks for a community value in the range of 30:100 to 30:500, in which case it sets the local-preference to 300.

```
RP/0/RP0/CPU0:router(config)# community-set my-community-set
RP/0/RP0/CPU0:router(config-comm)# 10:20,
RP/0/RP0/CPU0:router(config-comm)# 10:30,
RP/0/RP0/CPU0:router(config-comm)# 10:40
RP/0/RP0/CPU0:router(config-comm)# end-set

RP/0/RP0/CPU0:router(config)# route-policy community-matches-any-example
RP/0/RP0/CPU0:router(config-rpl)# if community matches-any my-community-set then
RP/0/RP0/CPU0:router(config-rpl)# set local-preference 100
RP/0/RP0/CPU0:router(config-rpl)# elseif community matches-any ([10..25]:35) then
RP/0/RP0/CPU0:router(config-rpl)# set local-preference 200
RP/0/RP0/CPU0:router(config-rpl)# elseif community matches-any (30:[100..500]) then
RP/0/RP0/CPU0:router(config-rpl)# set local-preference 300
RP/0/RP0/CPU0:router(config-rpl)# endif
RP/0/RP0/CPU0:router(config-rpl)# end-policy
```

Related Commands	Command	Description
	community matches-every	Matches every element of a community set.

R3.3 Beta Draft—Cisco Confidential Information

community matches-every

To match every element of a community set, use the **community matches-every** command in route-policy configuration mode.

community matches-every { *community-set-name* | *inline-community-set* }

Syntax Description

<i>community-set-name</i>	Name of a community set.
<i>inline-community-set</i>	Inline community set.

Defaults

No default behavior or values

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The BGP community matching operators were enhanced to allow comparisons on ranges and regular expressions.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **community matches-every** command as a conditional expression within an **if** statement to match every element of a community set.



Note

For a list of all conditional expressions available within an **if** statement, see the **if** command.

A simple condition using the **matches-every** operator evaluates as true if every specification in the named set or inline set specified matches at least one community value in the route. If any community specification in the named or inline set is not matched, then the operation evaluates to false. Therefore, a **matches-every** operation with two community range specifications means that a community must be present in the route that corresponds to each range. For example, in the following statement:

```
if community matches-every (10:[100..200],20:[100..200]) then
```

the statement evaluates as true if one or more communities in the route lie in the range 10:[100..200] and one or more communities in the route lie in the range 20:[100..200].

R3.3 Beta Draft—Cisco Confidential Information

Matching of a community in the route to a specification in a named or an inline set is intuitive. If the community-specification in a set is the familiar colon-separated decimal 16-bit numbers specification, or one of the well-known communities, the community matches the specification if the specification denotes the same 32-bit number as that in the route. If the community specification uses a wildcard, then the community in the route matches if it is one of the many communities denoted by the wildcard specification. In inline sets, community specifications may be parameterized, in which case the relevant matching is done when the value of the parameter has been supplied.

Communities may also be matched using range and regular expression operators. Range specifications are entered as follows: *[low-value..high-value]*. Either or both colon-separated halves of a community value may contain a range. The following are valid range specifications:

```
10:[100..1000]
[10..100]:80
[10..100]:[100..2000]
```

In addition, the **private-as** keyword may be used to specify the range from 64512 to 65534. Regular expressions are specified as the **ios-regex** keyword followed by a valid single-quoted regular expression string.

Community values from the route are matched one at a time against the match specifications. Therefore, regex match specifications are expected to represent one individual community value and not a sequence of community values.

Task ID	Task ID	Operations
	route-policy	read, write

Examples

In the following example, the route policy named community-matches-every-example sets the local-preference value to 100 for all routes that have all three communities in the my-community-set community set. Routes that do not have all three communities but have a community that matches the first regular expression match have the local-preference value set to 200. Finally, any remaining routes that match the last regular expression have the local-preference values set to 300.

```
RP/0/RP0/CPU0:router(config)# community-set my-community-set
RP/0/RP0/CPU0:router(config-comm)# 10:20,
RP/0/RP0/CPU0:router(config-comm)# 10:30,
RP/0/RP0/CPU0:router(config-comm)# 10:40
RP/0/RP0/CPU0:router(config-comm)# end-set

RP/0/RP0/CPU0:router(config)# route-policy community-matches-every-example
RP/0/RP0/CPU0:router(config-rpl)# if community matches-every my-community-set then
RP/0/RP0/CPU0:router(config-rpl)# set local-preference 100
RP/0/RP0/CPU0:router(config-rpl)# elseif community matches-every (ios-regex '_10:[0-9]0_')
then
RP/0/RP0/CPU0:router(config-rpl)# set local-preference 200
RP/0/RP0/CPU0:router(config-rpl)# elseif community matches-every (ios-regex '_20:[0-9]0_')
then
RP/0/RP0/CPU0:router(config-rpl)# set local-preference 300
RP/0/RP0/CPU0:router(config-rpl)# endif
RP/0/RP0/CPU0:router(config-rpl)# end-policy
```

Related Commands	Command	Description
	community matches-any	Matches any elements of a community set.

R3.3 Beta Draft—Cisco Confidential Information

community-set

To define a community set, use the **community-set** command in global configuration mode.

community-set *name*

no community-set *name*

Syntax Description

<i>name</i>	Name of the community set.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Regular expressions and ranges can be specified in a community set to support the matching or deleting of communities using ranges or regular expressions in named community sets. An attempt to use a community set that contains a range or regular expression to set a community value is rejected when an attempt to attach such a policy is made.

A community set holds community values for matching against the Border Gateway Protocol (BGP) community attribute. A community is a 32-bit quantity. For notational convenience, each community value must be split in half and expressed as two unsigned decimal integers in the range from 0 to 65535, separated by a colon.

The inline form of a community set also supports parameterization. Each 16-bit portion of the community may be parameterized.

The routing policy language (RPL) provides symbolic names for the standard well-known community values: **internet** is 0:0, **no-export** is 65535:65281, **no-advertise** is 65535:65282, and **local-as** is 65535:65283.

RPL also provides a facility for using wildcards in community specifications. A wildcard is specified by inserting an asterisk (*) in place of one of the 16-bit portions of the community specification, which indicates that any value for that portion of the community matches.

Every community set must contain at least one community value. An empty community set is invalid and the policy configuration system rejects it.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	route-policy	read, write

Examples

In the following example, a community set named cset1 is created:

```
RP/0/RP0/CPU0:router(config)# community-set cset1
RP/0/RP0/CPU0:router(config-comm)# 12:34,
RP/0/RP0/CPU0:router(config-comm)# 12:56,
RP/0/RP0/CPU0:router(config-comm)# 12:78,
RP/0/RP0/CPU0:router(config-comm)# internet
RP/0/RP0/CPU0:router(config-comm)# end-set
```

In the following example, a community set named cset2 is created:

```
RP/0/RP0/CPU0:router(config)# community-set cset2
RP/0/RP0/CPU0:router(config-comm)# 123:456,
RP/0/RP0/CPU0:router(config-comm)# no-advertise,
RP/0/RP0/CPU0:router(config-comm)# end-set
```

In the following example, a community set named cset3 is created. This policy uses wildcards and matches all communities where the autonomous system part of the community is 123.

```
RP/0/RP0/CPU0:router(config)# community-set cset3
RP/0/RP0/CPU0:router(config-comm)# 123:*
RP/0/RP0/CPU0:router(config-comm)# end-set
```

Related Commands	Command	Description
	extcommunity-set	Defines an extended community set.

R3.3 Beta Draft—Cisco Confidential Information

delete community

To delete community values from a community list in a route, use the **delete community** command in route-policy configuration mode.

delete community {**all** | **in** {*community-set-name* | *inline-community-set*} | **not in** {*community-set-name* | *inline-community-set*}}

Syntax Description		
all		Removes all communities except the well-known communities.
in		Removes any communities associated with the route that are listed in either the named community set or the inline community set.
not in		Removes all communities that are not listed in either the named community set or the inline community set, and are not well-known communities.
<i>community-set-name</i>		Name of a community set.
<i>inline-community-set</i>		Inline community set.

Defaults	No default behavior or values

Command Modes	Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The BGP community deletion operations were extended to allow communities that match a range specification or a regular expression to be deleted.
	Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **delete community** command to delete community values from a community list in a route.

**Note**

The **delete community** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

Communities are 32-bit values carried in Border Gateway Protocol (BGP) routes. Each route may have zero or more communities in an unordered list.

You can remove a well-known community (internet, no-export, no-advertise, or local-as) from a route, but this removal must be done explicitly. This command should be used with a degree of caution. In general, few circumstances exist in which you would need to remove a well-known community.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	route-policy	read, write

Examples

The following example shows how to delete any communities associated with the routes that are listed in either the named community set or inline community set, respectively.

```
RP/0/RP0/CPU0:router(config-rpl)# delete community in my_community_set
RP/0/RP0/CPU0:router(config-rpl)# delete community in (10:[0..50],20:[60..80])
```

The following example shows how to remove all communities except for the well-known communities.

```
RP/0/RP0/CPU0:router(config-rpl)# delete community all
```

The following example shows how to delete the well-known community value internet from a route:

```
RP/0/RP0/CPU0:router(config-rpl)# delete community in (internet)
```

R3.3 Beta Draft—Cisco Confidential Information

delete extcommunity

To delete extended community values from an extended community list in a route, use the **delete extcommunity** command in route-policy configuration mode.

```
delete extcommunity {all | in {extcommunity-set-name | inline-extcommunity-set} | not in
{extcommunity-set-name | inline-extcommunity-set}}
```

Syntax Description		
all		Removes all extended communities.
in		Removes any extended communities associated with the routes that are listed in either the named extended community set or the inline extended community set.
not in		Removes all extended communities that are not listed in either the named extended community set or the inline extended community set, and are not well-known extended communities.
<i>extcommunity-set-name</i>		Name of an extended community set.
<i>inline-extcommunity-set</i>		Inline extended community set.

Defaults No default behavior or values

Command Modes Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **delete extcommunity** command to delete extended community values from an extended community list in a route.



Note

The **delete extcommunity** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

Extended communities are similar to regular Border Gateway Protocol (BGP) communities but contain more data and have a richer structure for encoding information in them.

Extended communities can be in the following forms: SoO:AS:tag, SoO:IP:tag, RT:AS:tag, or RT:IP:tag.

R3.3 Beta Draft – Cisco Confidential Information

Wildcards (*) are not allowed for extended community set elements.

The forms of this command that take a named extended community set or an inline extended community set value as arguments are equivalent. They delete any extended communities that are listed in either the named set or the inline set, respectively.

Task ID	Task ID	Operations
	route-policy	read, write

Examples

In the following example, all extended communities are deleted:

```
RP/0/RP0/CPU0:router(config-rpl)# delete extcommunity all
```

In this example, any extended communities that are listed in my-extcommunity-set are deleted:

```
RP/0/RP0/CPU0:router(config-rpl)# delete extcommunity in my-extcommunity-set
```

In this example, extended communities associated with the route listed in the named inline extended community sets are deleted:

```
RP/0/RP0/CPU0:router(config-rpl)# delete extcommunity in (RT:67:29, RT:67:55)
```

R3.3 Beta Draft—Cisco Confidential Information

destination in

To match a destination entry in a named prefix set or inline prefix set, use the **destination in** command in route-policy configuration mode.

destination in {*prefix-set-name* | *inline-prefix-set*}

Syntax Description

<i>prefix-set-name</i>	Name of a prefix set.
<i>inline-prefix-set</i>	Inline prefix set.

Defaults

No default behavior or values

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **destination in** command as a conditional expression within an **if** statement to match a destination entry in a named prefix set or inline prefix set.



Note

For a list of all conditional expressions available within an **if** statement, see the **if** command.

This command takes either a named prefix set or an inline prefix set value as an argument. The condition returns true if the destination entry matches any entry in the prefix set or inline prefix set. An attempt to match a destination using a prefix set that is defined but contains no elements returns false.

The destination of a route is also known in Border Gateway Protocol (BGP) as its network-layer reachability information (NLRI). It comprises a prefix value and a mask length. The routing policy language (RPL) provides the ability to test destinations for a match to a list of prefix match specifications using the **in** operator.

RPL supports both 32-bit IPv4 prefixes, specified in dotted-decimal format, and 128-bit IPv6 prefixes, specified in colon-separated hexadecimal format.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	route-policy	read, write

Examples

In the following example, a prefix set named my-prefix-set is defined and a route policy named use-destination-in is created. Within the use-destination-in route policy, the **destination in** command is used within an **if** statement to learn if the destination is in the prefix-set named my-prefix-set. If it is, then local preference is set to 100. If it is not in my-prefix-set but does match the next prefix specifications, then local preference is set to 200.

```
RP/0/RP0/CPU0:router(config)# prefix-set my-prefix-set
RP/0/RP0/CPU0:router(config-pfx)# 10.0.0.1/32,
RP/0/RP0/CPU0:router(config-pfx)# fe80::203:0:0:0/64,
RP/0/RP0/CPU0:router(config-pfx)# 10.0.0.2/24 le 32
RP/0/RP0/CPU0:router(config-pfx)# end-set

RP/0/RP0/CPU0:router(config)# route-policy use-destination-in
RP/0/RP0/CPU0:router(config-rpl)# if destination in my-prefix-set then
RP/0/RP0/CPU0:router(config-rpl)# set local-preference 100
RP/0/RP0/CPU0:router(config-rpl)# elseif destination in (10.0.0.1/32, 10.0.0.2/24 le 32)
then
RP/0/RP0/CPU0:router(config-rpl)# set local-preference 200
RP/0/RP0/CPU0:router(config-rpl)# endif
RP/0/RP0/CPU0:router(config-rpl)# end-policy
```

In the following example, a prefix set named ipv6-prefix-set is defined and a route policy named ipv6-destination-in is created. Within the ipv6-destination-in route policy, the **destination in** command is used within an **if** statement to learn if the destination is in the prefix-set named ipv6-prefix-set. If it is, then the next hop is set to 2001:abcd:fedc::1. If it is not in ipv6-prefix-set but does match the next prefix specifications, then the next hop is set to 1111:2222:3333:4444:5555:6666:7777:8888.

```
RP/0/RP0/CPU0:router(config)# prefix-set ipv6-prefix-set
RP/0/RP0/CPU0:router(config-pfx)# 2001:0:0:1::/64,
RP/0/RP0/CPU0:router(config-pfx)# 2001:0:0:2::/64,
RP/0/RP0/CPU0:router(config-pfx)# 2001:0:0:3::/64,
RP/0/RP0/CPU0:router(config-pfx)# 2001:0:0:4::/64
RP/0/RP0/CPU0:router(config-pfx)# end-set

RP/0/RP0/CPU0:router(config)# route-policy ipv6-destination-in
RP/0/RP0/CPU0:router(config-rpl)# if destination in ipv6-prefix-set then
RP/0/RP0/CPU0:router(config-rpl)# set next-hop 2001:abcd:fedc::1
RP/0/RP0/CPU0:router(config-rpl)# elseif destination in (2001::1, 2002:1:2:3::/64) then
RP/0/RP0/CPU0:router(config-rpl)# set next-hop 1111:2222:3333:4444:5555:6666:7777:8888
RP/0/RP0/CPU0:router(config-rpl)# endif
RP/0/RP0/CPU0:router(config-rpl)# end-policy
```


R3.3 Beta Draft—Cisco Confidential Information

drop

To drop a route, use the **drop** command in route-policy configuration mode.

drop

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **drop** command within a route policy to drop a route.



Note

The **drop** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

This command signifies to the engine that executes policy that the action to take is to discard the route. After a route is dropped, no further execution of policy occurs. Therefore, if after executing the first two statements of a policy the **drop** statement is encountered, the route is discarded and execution stops immediately even when the policy contains further statements.



Note

The default action of a route policy is to drop or discard any routes that have not been either explicitly passed or attempted to be modified with an action. This action is in contrast to the route map model. In the route map model, the default drop action is taken for routes that do not successfully match any match clause in the route map. The routing policy language (RPL) does not have specific “match clauses,” which means the default drop behavior is controlled by whether a route has been explicitly passed or an attempt has been to modify the route using an action statement.

■ drop

R3.3 Beta Draft—Cisco Confidential Information

Task ID

Task ID	Operations
route-policy	read, write

Examples

In the following example, any route with a destination address contained within the prefix set pset1 is dropped:

```
RP/0/RP0/CPU0:router(config-rpl)# if destination in pset1 then  
RP/0/RP0/CPU0:router(config-rpl)# drop  
RP/0/RP0/CPU0:router(config-rpl)# endif
```

R3.3 Beta Draft—Cisco Confidential Information

edit

To edit the contents of a route policy, a prefix set, an AS path set, a community set, or an extended community set, use the **edit** command in EXEC mode.

edit { **route-policy** | **prefix-set** | **as-path-set** | **community-set** | **extended-community-set** } *name*

Syntax Description

route-policy	Edits the contents of a route policy.
prefix-set	Edits the contents of a prefix set.
as-path-set	Edits the contents of an AS path set.
community-set	Edits the contents of a community set.
extended-community-set	Edits the contents of an extended community set.
<i>name</i>	Name of a route policy, a prefix set, an AS path set, a community set, or an extended community set.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **edit** command to edit the contents of a route policy, a prefix set, an AS path set, a community set, or an extended community set.

After this command is entered, a copy of the route policy, prefix set, as path set, community set, or extended community set is moved to a temporary file and the editor is launched. After editing, save the changes by using the **save-buffer** command, C-X C-S (Control-X Control-S). To exit the editor, use the **quit** command, Control-X Control-C. When you quit the editor, the buffer is committed. If there are no parse errors, the configuration is committed.

Task ID

Task ID	Operations
route-policy	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

In the following example, the policy_A policy is opened in the editor:

```
RP/0/RP0/CPU0:router# edit route-policy policy_A
-----
== MicroEMACS 3.8b () == rpl_edit.139281 ==
  if destination in (2001::/8) then
    drop
  endif
end-policy
!

== MicroEMACS 3.8b () == rpl_edit.139281 ==
Parsing.
83 bytes parsed in 1 sec (82)bytes/sec
Committing.
1 items committed in 1 sec (0)items/sec
Updating.
Updated Commit database in 1 sec

RP/0/RP0/CPU0:router#
```

If there are parse errors, you are asked whether editing should continue:

```
RP/0/RP0/CPU0:router#edit route-policy policy_B
== MicroEMACS 3.8b () == rpl_edit.141738
route-policy policy_B
  set metric-type type_1
  if destination in (2001::/8) then
    drop
  endif
end-policy
!
== MicroEMACS 3.8b () == rpl_edit.141738 ==
Parsing.
105 bytes parsed in 1 sec (103)bytes/sec

% Syntax/Authorization errors in one or more commands.!! CONFIGURATION
FAILED DUE TO SYNTAX/AUTHORIZATION ERRORS
  set metric-type type_1
  if destination in (2001::/8) then
    drop
  endif
end-policy
!

Continue editing? [no]:
```

If you answer **yes**, the editor continues on the text buffer from where you left off. If you answer **no**, the running configuration is not changed and the editing session is ended.

After the policy is opened, it may be manipulated using normal editor commands, then saved and committed to the running configuration.

R3.3 Beta Draft—Cisco Confidential Information

end-policy

To end the definition of a route policy and exit route-policy configuration mode, use the **end-policy** command in route-policy configuration mode.

end-policy

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **end-policy** command to end the definition of a route policy and exit route-policy configuration mode.

Task ID	Task ID	Operations
	route-policy	read, write

Examples In the following example, the **end-policy** command ends the definition of a route policy:

```
RP/0/RP0/CPU0:router(config)# route-policy med-to-local-pref
RP/0/RP0/CPU0:router(config-rpl)# if med eq 150 then
RP/0/RP0/CPU0:router(config-rpl)# set local-preference 10
RP/0/RP0/CPU0:router(config-rpl)# elseif med eq 200 then
RP/0/RP0/CPU0:router(config-rpl)# set local-preference 60
RP/0/RP0/CPU0:router(config-rpl)# elseif med eq 250 then
RP/0/RP0/CPU0:router(config-rpl)# set local-preference 0
RP/0/RP0/CPU0:router(config-rpl)# endif
RP/0/RP0/CPU0:router(config-rpl)# end-policy
```

R3.3 Beta Draft—Cisco Confidential Information

end-set

To end the definition of an AS path set, a prefix set, a community set, an extended community set or an RD set and return to global configuration mode, use the **end-set** command in route-policy configuration mode.

end-set

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	Added support functionality for the rd-set command.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **end-set** command to end the definition of an AS path set, a prefix set, a community set, or an extended community set.

Task ID

Task ID	Operations
route-policy	read, write

Examples

In the following example, the **end-set** command ends the definition of an AS path set named aset1:

```
RP/0/RP0/CPU0:router(config)# as-path-set aset1
RP/0/RP0/CPU0:router(config-as)# ios-regex '_42$',
RP/0/RP0/CPU0:router(config-as)# ios-regex '_127$'
RP/0/RP0/CPU0:router(config-as)# end-set
RP/0/RP0/CPU0:router(config)#
```

R3.3 Beta Draft—Cisco Confidential Information

extcommunity rt is-empty

To test to learn if a Border Gateway Protocol (BGP) route target (RT) has extended community attributes associated with it, use the **extcommunity rt is-empty** command in route-policy configuration mode.

extcommunity rt is-empty

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or value

Command Modes Route-policy configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router. This command replaced the extcommunity is-empty command.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **extcommunity rt is-empty** command as a conditional expression within an **if** statement to learn if a BGP route has extended community attributes associated with it.



Note

For a list of all conditional expressions available within an **if** statement, see the **if** command.

The **is-empty** operator takes no arguments and evaluates to true if the route has no extended community attributes associated with it.

Task ID	Task ID	Operations
	route-policy	read, write

Examples In the following example, if the extended community is empty, then the local preference is set to 100:

```
RP/0/RP0/CPU0:router(config)# route-policy extcommunity-is-empty-example
RP/0/RP0/CPU0:router(config-rpl)# if extcommunity rt is-empty then
RP/0/RP0/CPU0:router(config-rpl)# set local-preference 100
RP/0/RP0/CPU0:router(config-rpl)# endif
RP/0/RP0/CPU0:router(config-rpl)# end-policy
```

R3.3 Beta Draft—Cisco Confidential Information

extcommunity rt matches-any

To match any elements of a Border Gateway Protocol (BGP) route target (RT) extended community set, use the **extcommunity rt matches-any** command in route-policy configuration mode.

extcommunity rt matches-any {*extcommunity-set-name* | *inline-extcommunity-set*}

Syntax Description

<i>extcommunity-set-name</i>	Name of an extended community set.
<i>inline-extcommunity-set</i>	Inline extended community set.

Defaults

No default behavior or values

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router. This command replaced the extcommunity matches-any command.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **extcommunity rt matches-any** command as a conditional expression within an **if** statement to match elements of an extended community set.

**Note**

For a list of all conditional expressions available within an **if** statement, see the **if** command.

A simple condition using the **matches-any** operator evaluates as true if at least one extended community in the route matches an extended community specification in the named or inline set. If no extended community in the route matches any of the specifications in the named or inline set, then this simple condition evaluates to false. Likewise, when there is no extended community at all in the route, the condition evaluates to false.

Matching an extended community in the route to a specification in a named or an inline set is intuitive. Because there is no use of wildcards with extended communities, a community in the route matches a specification in the set if they encode the same 64-bit number. In inline sets, extended community specifications may be parameterized, in which case the relevant matching is done when the value of the parameter has been supplied.

Task ID

Task ID	Operations
route-policy	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples TBD

Related Commands	Command	Description
	extcommunity rt matches-every	Matches every element of a BGP RT extended community set.

R3.3 Beta Draft—Cisco Confidential Information

extcommunity rt matches-every

To match every element of a Border Gateway Protocol (BGP) route target (RT) extended community set, use the **extcommunity rt matches-every** command in route-policy configuration mode.

extcommunity rt matches-every {*extcommunity-set-name* | *inline-extcommunity-set*}

Syntax Description

<i>extcommunity-set-name</i>	Name of an extended community set.
<i>inline-extcommunity-set</i>	Inline extended community set.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router. This command replaced the extcommunity matches-every command.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **extcommunity rt matches-every** command as a conditional expression within an **if** statement to match every element of an extended community set.

**Note**

For a list of all conditional expressions available within an **if** statement, see the **if** command.

A simple condition using the **matches-every** operator evaluates as true if every extended community value in the extended community attribute for the route matches at least one element of the extended community set or inline set. If no extended community in the route matches any of the specifications in the named or inline set, then this simple condition evaluates to false. Likewise, when there is no extended community at all in the route, the condition evaluates to false.

Matching an extended community in the route to a specification in a named or an inline set is intuitive. Because there is no use of wildcards with extended communities, a community in the route matches a specification in the set if they encode the same 64-bit number. In inline sets, extended community specifications may be parameterized, in which case the relevant matching is done when the value of the parameter has been supplied.

Task ID

Task ID	Operations
route-policy	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples TBD

Related Commands	Command	Description
	extcommunity rt matches-any	Matches any element of a BGP RT extended community set.

R3.3 Beta Draft—Cisco Confidential Information

extcommunity-set

To define an extended community set, use the **extcommunity-set** command in global configuration mode.

extcommunity-set *name*

no extcommunity-set *name*

Syntax Description

<i>name</i>	Name of an extended community set.

Defaults

No default behavior or value

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **extcommunity-set** command to define an extended community set.

This command enters extcommunity-set configuration mode, where you can define extended community values with the following commands:

- **rt:a.b.c.d:n**—Border Gateway Protocol (BGP) route target (RT) extended community in IPv4 format. For example, rt:10.0.0.2:666.
- **rt:asn:n**—BGP RT extended community in ASN format. For example, rt:10002:666.
- **SoO:a.b.c.d:n**—BGP site of origin (SoO) extended community in IPv4 format. For example, SoO:10.0.0.5:777.
- **SoO:asn:n**—BGP SoO extended community in ASN format. For example, SoO:10005:777.

An extended community set is analogous to a community set except that it contains extended community values instead of regular community values. Extended community values are 64-bit structured values. An extended community set also supports named forms and inline forms.

As with community sets, the inline form supports parameterization within parameterized policies. Either portion of the extended community value can be parameterized.

Every extended community set must contain at least one extended community value. Empty extended community sets are invalid and the policy configuration system rejects them.

R3.3 Beta Draft – Cisco Confidential Information

**Note**

Parameterization of the extended community type RT and SoO is not supported. Making wildcards of extended communities is also not currently supported.

Examples

In the following example, an extended community set named extcomm-set1 is defined:

```
RP/0/RP0/CPU0:router(config)# extcommunity-set extcomm-set1
RP/0/RP0/CPU0:router(config-ext)# rt:1.2.3.4:666,
RP/0/RP0/CPU0:router(config-ext)# rt:1234:666,
RP/0/RP0/CPU0:router(config-ext)# SoO:1.2.3.4:777,
RP/0/RP0/CPU0:router(config-ext)# SoO:4567:777
RP/0/RP0/CPU0:router(config-ext)# end-set
```

Related Commands

Command	Description
community-set	Defines a community set.

R3.3 Beta Draft – Cisco Confidential Information**extcommunity-set cost**

TBD

|
|

R3.3 Beta Draft—Cisco Confidential Information**extcommunity-set rt**

TBD

R3.3 Beta Draft – Cisco Confidential Information**extcommunity-set soo**

TBD

|
|

R3.3 Beta Draft—Cisco Confidential Information

ext-community soo is-empty

To test to learn if a Border Gateway Protocol (BGP) Site-of-Origin extended community has attributes associated with it, use the **extcommunity soo is-empty** command in route-policy configuration mode.

extcommunity soo is-empty

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router. This command replaced the extcommunity is-empty command.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **extcommunity soo is-empty** command as a conditional expression within an **if** statement to learn if a BGP SoO route has extended community attributes associated with it.

**Note**

For a list of all conditional expressions available within an **if** statement, see the **if** command.

The **is-empty** operator takes no arguments and evaluates to true if the route has no extended community attributes associated with it.

Task ID

Task ID	Operations
route-policy	read, write

Examples

In the following example, if the extended community is empty, then the local preference is set to 100:

```
RP/0/RP0/CPU0:router(config)# route-policy extcommunity-is-empty-example
RP/0/RP0/CPU0:router(config-rpl)# if extcommunity soo is-empty then
RP/0/RP0/CPU0:router(config-rpl)# set local-preference 100
RP/0/RP0/CPU0:router(config-rpl)# endif
RP/0/RP0/CPU0:router(config-rpl)# end-policy
```

R3.3 Beta Draft—Cisco Confidential Information

ext-community soo matches-any

To match any elements of a Border Gateway Protocol (BGP) Site-of-Origin extended community set, use the **extcommunity soo matches-any** command in route-policy configuration mode.

extcommunity soo matches-any {*extcommunity-set-name* | *inline-extcommunity-set*}

Syntax Description

<i>extcommunity-set-name</i>	Name of an extended community set.
<i>inline-extcommunity-set</i>	Inline extended community set.

Defaults

No default behavior or values

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router. This command replaced the extcommunity matches-any command.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **extcommunity soo matches-any** command as a conditional expression within an **if** statement to match elements of an extended community set.

**Note**

For a list of all conditional expressions available within an **if** statement, see the **if** command.

A simple condition using the **matches-any** operator evaluates as true if at least one extended community in the route matches an extended community specification in the named or inline set. If no extended community in the route matches any of the specifications in the named or inline set, then this simple condition evaluates to false. Likewise, when there is no extended community at all in the route, the condition evaluates to false.

Matching an extended community in the route to a specification in a named or an inline set is intuitive. Because there is no use of wildcards with extended communities, a community in the route matches a specification in the set if they encode the same 64-bit number. In inline sets, extended community specifications may be parameterized, in which case the relevant matching is done when the value of the parameter has been supplied.

Task ID

Task ID	Operations
route-policy	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples TBD

Related Commands	Command	Description
	extcommunity rt matches-every	Matches every element of a BGP RT extended community set.

R3.3 Beta Draft—Cisco Confidential Information

ext-community soo matches-every

To match every element of a Border Gateway Protocol (BGP) Site-of-Origin extended community set, use the **extcommunity soo matches-every** command in route-policy configuration mode.

extcommunity soo matches-every {*extcommunity-set-name* | *inline-extcommunity-set*}

Syntax Description

<i>extcommunity-set-name</i>	Name of an extended community set.
<i>inline-extcommunity-set</i>	Inline extended community set.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router. This command replaced the extcommunity matches-every command.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **extcommunity soo matches-every** command as a conditional expression within an **if** statement to match every element of an extended community set.

**Note**

For a list of all conditional expressions available within an **if** statement, see the **if** command.

A simple condition using the **matches-every** operator evaluates as true if every extended community value in the extended community attribute for the route matches at least one element of the extended community set or inline set. If no extended community in the route matches any of the specifications in the named or inline set, then this simple condition evaluates to false. Likewise, when there is no extended community at all in the route, the condition evaluates to false.

Matching an extended community in the route to a specification in a named or an inline set is intuitive. Because there is no use of wildcards with extended communities, a community in the route matches a specification in the set if they encode the same 64-bit number. In inline sets, extended community specifications may be parameterized, in which case the relevant matching is done when the value of the parameter has been supplied.

Examples

TBD

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	<code>ext-community soo matches-any</code>	Matches any elements of a BGP SoO extended community set.

R3.3 Beta Draft—Cisco Confidential Information

if

To decide which actions or dispositions should be taken for a given route, use the **if** command in route-policy configuration mode.

```
if conditional-expression then action-statement [action-statement] [elseif conditional-expression
then action-statement [action-statement]] [else action-statement [action-statement]] endif
```

Syntax Description

<i>conditional-expression</i>	Expression to decide which actions or dispositions should be taken for the given route.
then	Executes an action statement if the if condition is true.
elseif	Strings together a sequence of tests.
else	Executes an action statement if the if condition is false.
endif	Ends the if statement.
<i>action-statement</i>	Sequence of operations that modify a route.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **if** command uses a conditional expression to decide which actions or dispositions should be taken for a given route. [Table 131](#) lists the conditional expressions.

An action statement is a sequence of operations that modify a route, most of which are distinguished by the **set** keyword. In a route policy, these operations can be grouped. [Table 132](#) lists the conditional expressions.

R3.3 Beta Draft – Cisco Confidential Information

Table 131 **Conditional Expressions**

Command	Description
as-path in	Matches the AS path of a route to an AS path set. The AS path is a sequence of autonomous system numbers traversed by a route.
as-path is-local	Determines if the router (or another router within this autonomous system or confederation) originated the route.
as-path length	Performs a conditional check based on the length of the AS path.
as-path neighbor-is	Tests the autonomous system number or numbers at the head of the AS path against a sequence of one or more integral values or parameters.
as-path originates-from	Compares an AS path to the autonomous system sequence.
as-path passes-through	Tests to learn if the specified integer or parameter appears anywhere in the AS path or if the sequence of integers and parameters appears.
as-path unique-length	Performs specific checks based on the length of the AS path.
community is-empty	Learns if a route has community attributes associated with it.
community matches-any	Matches any element of a community set.
community matches-every	Matches every element of a community set.
destination in	Matches a destination entry in a named prefix set or inline prefix set.
extcommunity rt is-empty	Learns if a route has RT extended community attributes associated with it.
extcommunity rt matches-any	Matches elements of an RT extended community set.
extcommunity rt matches-every	Matches every element of an RT extended community set.
ext-community soo is-empty	Learns if a route has SoO extended community attributes associated with it.
ext-community soo matches-any	Matches elements of an SoO extended community set.
ext-community soo matches-every	Matches every element of an SoO extended community set.
med	Compares the MED to an integer value or a parameterized value.
next-hop in	Compares the next hop associated with the route to data contained in either a named or an inline prefix set.
origin is	Tests the value of the origin attribute.
protocol	Checks if a protocol is installing the route.
rd in	Compares the RD associated with the route to data contained in either a named or inline RD set.
rib-has-route	Checks if a RIB is in a route.

R3.3 Beta Draft—Cisco Confidential Information

Table 131 *Conditional Expressions (continued)*

Command	Description
route-type is	Compares route types when redistribution is being performed into BGP, OSPF, or IS-IS.
source in	Tests the source of the route against the data in either a named or an inline prefix set.
tag	Matches a specific tag value.

Table 132 *Action Statements*

Command	Description
delete community	Deletes community values from a community list in a route.
delete extcommunity	Deletes extended community values from an extended community list in a route.
drop	Drops a route.
pass	Signifies that even though the route has not been modified, the user wants to continue executing in the policy block.
prepend as-path	Prepends the AS path with additional autonomous system numbers.
set community	Sets the BGP community attribute.
set cost	Sets the cost attribute for routes that are redistributed into OSPF.
set dampening	Configures BGP route dampening.
set extcommunity	Replaces or adds the extended communities on the route.
set level	Configures the IS-IS level in which redistributed routes should be sent.
set local-preference	Specifies a preference value for the autonomous system path.
set med	Sets the MED value.
set metric	Configures the link metric of routes that are redistributed into IS-IS.
set metric-type (IS-IS)	Controls whether IS-IS treats the metric as an internal or external metric.
set metric-type (OSPF)	Controls whether OSPF treats the cost as a Type 1 or Type 2 metric.
set next-hop	Replaces the next hop associated with a given route.
set origin	Changes the origin attribute.
set tag	Sets the tag attribute.
set traffic-index	Sets the traffic index attribute.

R3.3 Beta Draft—Cisco Confidential Information

Table 132 Action Statements (continued)

Command	Description
set weight	Sets the weight value for BGP routes.
suppress-route	Indicates that a given component of an aggregate should be suppressed, that is, not advertised.

Task ID

Task ID	Operations
route-policy	read, write

Examples

In the following example, any route whose AS path is in the set as-path-set-1 is dropped:

```
RP/0/RP0/CPU0:router(config-rpl)# if as-path in as-path-set-1 then
RP/0/RP0/CPU0:router(config-rpl-if)# drop
RP/0/RP0/CPU0:router(config-rpl-if)# endif
```

The contents of the **then** clause may be an arbitrary sequence of action statements.

The following example shows an **if** statement with two action statements:

```
RP/0/RP0/CPU0:router(config-rpl)# if origin is igp then
RP/0/RP0/CPU0:router(config-rpl-if)# set med 42
RP/0/RP0/CPU0:router(config-rpl-if)# prepend as-path 73 5
RP/0/RP0/CPU0:router(config-rpl-if)# endif
```

The **if** command also permits an **else** clause to be executed if the expression is false, as follows:

```
RP/0/RP0/CPU0:router(config-rpl)# if med eq 200 then
RP/0/RP0/CPU0:router(config-rpl-if)# set community (12:34) additive
RP/0/RP0/CPU0:router(config-rpl-if)# else
RP/0/RP0/CPU0:router(config-rpl-if)# set community (12:56) additive
RP/0/RP0/CPU0:router(config-rpl-if)# endif
```

The routing policy language (RPL) also provides syntax using the **elseif** command to string together a sequence of tests, as shown in the following example:

```
RP/0/RP0/CPU0:router(config-rpl)# if med eq 150 then
RP/0/RP0/CPU0:router(config-rpl-if)# set local-preference 10
RP/0/RP0/CPU0:router(config-rpl-if)# elseif med eq 200 then
RP/0/RP0/CPU0:router(config-rpl-if)# set local-preference 60
RP/0/RP0/CPU0:router(config-rpl-if)# elseif med eq 250 then
RP/0/RP0/CPU0:router(config-rpl-if)# set local-preference 110
RP/0/RP0/CPU0:router(config-rpl-if)# else
RP/0/RP0/CPU0:router(config-rpl-if)# set local-preference 0
RP/0/RP0/CPU0:router(config-rpl-if)# endif
```

The statements within an **if** statement may themselves be **if** statements, as shown in this example:

```
RP/0/RP0/CPU0:router(config-rpl)# if community matches-any (12:34, 56:78) then
RP/0/RP0/CPU0:router(config-rpl-if)# if med eq 150 then
RP/0/RP0/CPU0:router(config-rpl-if)# drop
RP/0/RP0/CPU0:router(config-rpl-if)# endif
RP/0/RP0/CPU0:router(config-rpl-if)# set local-preference 100
RP/0/RP0/CPU0:router(config-rpl-if)# endif
```

R3.3 Beta Draft – Cisco Confidential Information

The policy configuration shown sets the value of the local preference attribute to 100 on any route that has a community value of 12:34 or 56:78 associated with it. However, if any of these routes has a Multi Exit Discriminator (MED) value of 150, then each route with both the community value of 12:34 or 56:78 and a MED of 150 is dropped.

R3.3 Beta Draft—Cisco Confidential Information**med**

To compare the Multi Exit Discriminator (MED) to an integer value or a parameterized value, use the **med** command in route-policy configuration mode.

```
med {eq | is | ge | le} {integer | parameter}
```

Syntax Description	eq is ge le	Equal to; greater than or equal to; less than or equal to.
	integer	Integer value to compare to the MED. Range is 0 to 4294967295.
	parameter	Parameter value to compare to the MED.

Defaults	No default behavior or value

Command Modes	Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

Use the **med** command as a conditional expression within an **if** statement to compare the MED to an integer value or a parameterized value.

**Note**

For a list of all conditional expressions available within an **if** statement, see the **if** command.

The MED is a 32-bit unsigned integer. The **eq** operation compares the MED to either a static value or a parameterized value passed to a parameterized policy for equality with that value. A greater than or equal to comparison can also be done with the **ge** operator, and a less than or equal to comparison can be performed using the **le** operator.

Task ID	Task ID	Operations
	route-policy	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows that if the **med** commands match, the local preference is set to 100:

```
RP/0/RP0/CPU0:router(config-rpl)# if med eq 10 then
RP/0/RP0/CPU0:router(config-rpl)# if med eq $med then
RP/0/RP0/CPU0:router(config-rpl)# if med ge 10 then
RP/0/RP0/CPU0:router(config-rpl)# if med ge $med then
RP/0/RP0/CPU0:router(config-rpl)# if med le 10 then
RP/0/RP0/CPU0:router(config-rpl)# if med le $med then
RP/0/RP0/CPU0:router(config-rpl-if)# set local-preference 100
RP/0/RP0/CPU0:router(config-rpl-if)# endif
```

R3.3 Beta Draft—Cisco Confidential Information

next-hop in

To compare the next hop associated with the route to data contained in either an inline or a named prefix set, use the **next-hop in** command in route-policy configuration mode.

next-hop in {*prefix-set-name* | *inline-prefix-set*}

Syntax Description

<i>prefix-set-name</i>	Name of a prefix set.
<i>inline-prefix-set</i>	Inline prefix set.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **next-hop in** command as a conditional expression within an **if** statement to compare the next hop associated with the route to data contained in either an inline or a named prefix set. The result is true if any value in the prefix set matches the next hop of the route. A comparison that refers to a named prefix set that has no elements in it returns false.



Note

For a list of all conditional expressions available within an **if** statement, see the **if** command.

The next hop is an IPv4 address entered as a dotted decimal or an IPv6 address entered as a colon-separated hexadecimal.

Task ID

Task ID	Operations
route-policy	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows that if the **next-hop in** commands match, the local preference is set to 100

```
RP/0/RP0/CPU0:router(config-rpl)# if next-hop in some-prefix-set then
RP/0/RP0/CPU0:router(config-rpl-if)# if next-hop in (10.0.0.5, fe80::230/64) then
RP/0/RP0/CPU0:router(config-rpl-if)# set local-preference 0
RP/0/RP0/CPU0:router(config-rpl-if)# endif
```

R3.3 Beta Draft—Cisco Confidential Information

origin is

To match a specific origin type, use the **origin is** command in route-policy configuration mode.

origin is { **igp** | **egp** | **incomplete** | *parameter* }

Syntax Description	igp	Specifies Interior Gateway Protocol.
	egp	Specifies Exterior Gateway Protocol.
	incomplete	Specifies that Border Gateway Protocol (BGP) first learned the route by means other than BGP or Interior Gateway Protocol (IGP); for example, the route is learned through configuration.
	<i>parameter</i>	Parameter name. The parameter name must be preceded with a "\$."

Defaults	No default behavior or value

Command Modes	Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **origin is** command as a conditional expression within an **if** statement to test the value of the origin attribute.

**Note**

For a list of all conditional expressions available within an **if** statement, see the **if** command.

The origin of a BGP route is an enumeration; it is **igp**, **egp**, or **incomplete**.

This command can be parameterized.

Task ID	Task ID	Operations
	route-policy	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

In the following example, the origin is tested within an **if** statement to learn if it is either **igp** or **egp**:

```
RP/0/RP0/CPU0:router(config-rpl)# if origin is igp or origin is egp then
```

In the following example, a parameter is used to match a specific origin type:

```
RP/0/RP0/CPU0:router(config)# route-policy bar($origin)
RP/0/RP0/CPU0:router(config-rpl)# if origin is $origin then
RP/0/RP0/CPU0:router(config-rpl-if)# set med 20
RP/0/RP0/CPU0:router(config-rpl-if)# endif
RP/0/RP0/CPU0:router(config-rpl-if)# end policy
```


R3.3 Beta Draft—Cisco Confidential Information

pass

To pass a route for further processing, use the **pass** command in route-policy configuration mode.

pass

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or value

Command Modes Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **pass** command to signify that even though this route has not been modified, the user wants to continue executing in this policy block.

**Note**

The **pass** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

When a policy block has finished executing, any route that has been modified in this policy block or has received a pass disposition in this policy block passes the policy and execution finishes for that policy. If this policy block is applied from within another policy block and the route is either passed or modified, then execution continues in the policy block that applied this policy block.

Task ID	Task ID	Operations
	route-policy	read, write

Examples The following example shows how to accept the route unconditionally, without modifying it:

```
RP/0/RP0/CPU0:router(config-rpl)# pass
```

 pass

R3.3 Beta Draft – Cisco Confidential Information

This example accepts the route unconditionally, without modifying it, if the destination is in prefix-set permitted:

```
RP/0/RP0/CPU0:router(config-rpl)# if destination in permitted then  
RP/0/RP0/CPU0:router(config-rpl-if)# pass  
RP/0/RP0/CPU0:router(config-rpl-if)# endif
```

R3.3 Beta Draft—Cisco Confidential Information

prefix-set

To define a prefix set, use the **prefix-set** command in global configuration mode. To remove a named prefix set, use the **no** form of this command.

prefix-set *name*

no prefix-set *name*

Syntax Description

<i>name</i>	Name of a prefix set.

Defaults

No default behavior or value

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **prefix-set** command to define a prefix set.

A prefix set is a comma-separated list of prefix match specifications. It holds IPv4 or IPv6 prefix match specifications, each of which has four parts: an address, a mask length, a minimum matching length, and a maximum matching length. The address is required, but the other three parts are optional. The address is a standard four-part, dotted-decimal numeric IPv4 address or a colon-separated hexadecimal IPv6 address. The mask length, if present, is a nonnegative decimal integer in the range from 0 to 32 for IPv4 prefixes or 0 to 128 for IPv6 prefixes following the address and separated from it by a slash. The optional minimum matching length follows the address and optional mask length and is expressed as the keyword **ge** (mnemonic for **g**reater than or **e**qual to), followed by a nonnegative decimal integer in the range from 0 to 32 for IPv4 or 0 to 128 for IPv6. The optional maximum matching length follows the rest and is expressed by the keyword **le** (mnemonic for **l**ess than or **e**qual to), followed by yet another nonnegative decimal integer in the range from 0 to 32 for IPv4 or 0 to 128 for IPv6. A syntactic shortcut for specifying an exact length for prefixes to match is the **eq** keyword, mnemonic for **e**qual to.

If a prefix match specification has no mask length, then the default mask length is 32 for IPv4 or 128 for IPv6. The default minimum matching length is the mask length. If a minimum matching length is specified, then the default maximum matching length must be less than 32 for IPv4 prefixes or 128 for IPv6 prefixes. Otherwise, if neither a minimum nor maximum length is specified, the default maximum length is the mask length.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	route-policy	read, write

Examples

The following example shows a prefix set named legal-ipv4-prefix-examples:

```
RP/0/RP0/CPU0:router(config)# prefix-set legal-ipv4-prefix-examples
RP/0/RP0/CPU0:router(config-pfx)# 10.0.1.1,
RP/0/RP0/CPU0:router(config-pfx)# 10.0.2.0/24,
RP/0/RP0/CPU0:router(config-pfx)# 10.0.3.0/24 ge 28,
RP/0/RP0/CPU0:router(config-pfx)# 10.0.4.0/24 le 28,
RP/0/RP0/CPU0:router(config-pfx)# 10.0.5.0/24 ge 26 le 30,
RP/0/RP0/CPU0:router(config-pfx)# 10.0.6.0/24 eq 28
RP/0/RP0/CPU0:router(config-pfx)# end-set
```

The first element of the prefix set matches only one possible value, 10.0.1.1/32 or the host address 10.0.1.1. The second element matches only one possible value, 10.0.2.0/24. The third element matches a range of prefix values, from 10.0.3.0/28 to 10.0.3.255/32. The fourth element matches a range of values, from 10.0.4.0/24 to 10.0.4.240/28. The fifth element matches prefixes in the range from 10.0.5.0/26 to 10.0.5.252/30. The sixth element matches any prefix of length 28 in the range from 10.0.6.0/28 through 10.0.6.240/28.

The following prefix set consists entirely of invalid prefix match specifications:

```
RP/0/RP0/CPU0:router(config)# prefix-set INVALID-PREFIX-EXAMPLES
RP/0/RP0/CPU0:router(config-pfx)# 10.1.1.1 ge 16,
RP/0/RP0/CPU0:router(config-pfx)# 10.1.2.1 le 16,
RP/0/RP0/CPU0:router(config-pfx)# 10.1.3.0/24 le 23,
RP/0/RP0/CPU0:router(config-pfx)# 10.1.4.0/24 ge 33,
RP/0/RP0/CPU0:router(config-pfx)# 10.1.5.0/25 ge 29 le 28
RP/0/RP0/CPU0:router(config-pfx)# end-set
```

Neither the minimum length nor the maximum length is legal without a mask length. The maximum length must be at least the mask length. The minimum length must be less than 32, the maximum length of an IPv4 prefix. The maximum length must be equal to or greater than the minimum length.

The following example shows a valid IPv6 prefix set named legal-ipv6-prefix-examples:

```
RP/0/RP0/CPU0:router(config)# prefix-set legal-ipv6-prefix-examples
RP/0/RP0/CPU0:router(config-pfx)# 2001:0:0:1::/64,
RP/0/RP0/CPU0:router(config-pfx)# 2001:0:0:2::/64,
RP/0/RP0/CPU0:router(config-pfx)# 2001:0:0:3::/64,
RP/0/RP0/CPU0:router(config-pfx)# 2001:0:0:4::/64
RP/0/RP0/CPU0:router(config-pfx)# end-set
```

R3.3 Beta Draft—Cisco Confidential Information

prepend as-path

To prepend the AS path with additional autonomous system numbers, use the **prepend as-path** command in route-policy configuration mode.

prepend as-path {*as-number* | *parameter*} [*prepend-number* | *parameter*]

Syntax Description

<i>as-number</i>	Autonomous system number to prepend to the path.
<i>parameter</i>	Parameter value.
<i>prepend-number</i>	(Optional) Number of times the autonomous system number should be prepended.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **prepend as-path** command to prepend the AS path with additional autonomous system numbers.



Note

The **prepend as-path** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

This command can take one or two arguments. The first argument (either a number or parameter) is the autonomous system number to prepend to the path. The optional second argument (either a number or parameter) is the number of times the autonomous system number should be prepended.

Task ID

Task ID	Operations
route-policy	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

The following example shows how to prepend the autonomous system number 666 to the AS path three times:

```
RP/0/RP0/CPU0:router(config-rpl)# prepend as-path 666 3
```

The following example shows how to prepend the autonomous system number 666 to the AS path one time:

```
RP/0/RP0/CPU0:router(config-rpl)# prepend as-path 666
```

R3.3 Beta Draft—Cisco Confidential Information

protocol

To check the protocol that installs the route, use the **protocol** command in route-policy configuration mode.

protocol {**in** | **is**}

Syntax Description

in	Specifies a member of a set.
is	Specifies an exact match.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **protocol** command as a conditional expression within an if statement to specify a protocol to install a route.



Note

For a list of all conditional expressions available within an **if** statement, see the **if** command.

Task ID

Task ID	Operations
route-policy	read, write

Examples

```
!  
route-policy test-rip  
  if protocol in (connected, static) then  
    add rip-metric 2  
  elseif protocol is bgp 1 then  
    add rip-metric 3  
  elseif protocol is ospf 2 then  
    add rip-metric 4  
  else  
    add rip-metric 5  
  endif  
end-policy
```

R3.3 Beta Draft – Cisco Confidential Information

```
!  
router rip  
  interface GigabitEthernet0/1/0/1  
    route-policy test-rip out  
  !
```


R3.3 Beta Draft—Cisco Confidential Information

rd in

To compare the route distinguisher (RD) associated with the route to data contained in either a named or inline RD set, use the **rd in** command in route-policy configuration mode.

```
rd in {rd-set-name | inline-rd-set}
```

Syntax Description

<i>rd-set-name</i>	Name of an RD set.
<i>inline-rd-set</i>	Inline RD set.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **rd in** command as a conditional expression within an **if** statement to match a destination entry in a named prefix set or inline prefix set.



Note

For a list of all conditional expressions available within an **if** statement, see the **if** command.

This command takes either a named RD set or an inline RD set value as an argument. The condition returns true if the destination entry matches any entry in the RD set or inline RD set. An attempt to match an RD using an RD set that is defined but contains no elements returns false.

Task ID

Task ID	Operations
route-policy	read, write

Examples

The following sample uses the **rd in** command with an inline RD set value as an argument:

```
RP/0/RP0/CPU0:router(config)# route-policy
RP/0/RP0/CPU0:router(config-rpl)# if rd in (128.1.0.0/16:100) then
RP/0/RP0/CPU0:router(config-rpl-if)# pass
RP/0/RP0/CPU0:router(config-rpl-if)# endif
RP/0/RP0/CPU0:router(config-rpl-if)# end-policy
```

R3.3 Beta Draft—Cisco Confidential Information

rd-set

To define a route distinguisher (RD) set and enter RD configuration mode, use the **rd-set** command in global configuration mode.

rd-set *name*

no rd-set *name*

Syntax Description	<i>name</i>	Name of an RD community set.

Defaults	No default behavior or value

Command Modes	Global configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **rd-set** command to create a set with RD elements and enter RD configuration mode. An RD set is a 64-bit value prepended to an IPv4 address to create a globally unique Border Gateway Protocol (BGP) VPN-IPv4 address.

You can define RD values with the following commands:

- *a.b.c.d:m:**—BGP VPN RD in IPv4 format with wildcard character. For example, 10.0.0.2:255.255.0.0:*
- *a.b.c.d/m:n*—BGP VPN RD in IPv4 format with mask. For example, 10.0.0.2:255.255.0.0:666.
- *a.b.c.d:** —BGP VPN RD in IPv4 format with wildcard character. For example, 10.0.0.2:255.255.0.0.
- *a.b.c.d:n* —BGP VPN RD in IPv4 format. For example, 10.0.0.2:666.
- *asn:**—BGP VPN RD in ASN format with wildcard character. For example, 10002:255.255.0.0.
- *asn:n*—BGP VPN RD in ASN format. For example, 10002:666.

Task ID	Task ID	Operations
	route-policy	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following example shows how to create an RD set called my_rd_set:

```
RP/0/RP0/CPU0:router(config)# rd-set my_rd_set  
RP/0/RP0/CPU0:router(config-rd)# 172.16.0.0/16:*,  
RP/0/RP0/CPU0:router(config-rd)# 172.17.0.0/16:100,  
RP/0/RP0/CPU0:router(config-rd)# 192:*,  
RP/0/RP0/CPU0:router(config-rd)# 192:100  
RP/0/RP0/CPU0:router(config-rd)# end-set
```

R3.3 Beta Draft—Cisco Confidential Information

rib-has-route

To check if there is a Routing Information Base (RIB) in a route, use the **rib-has-route** command in route-policy configuration mode.

rib-has-route in *rib_name*

Syntax Description	<i>rib_name</i> RIB name.

Defaults	No default behavior or value

Command Modes	Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **rib-has-route** command as a conditional expression within an **if** statement to check if there is a RIB in a route.

For a list of all conditional expressions available within an **if** statement, see the **if** command.

Task ID	Task ID	Operations
	route-policy	read, write

Examples	In the following example, an if statement is used to learn if a RIB named pf1 is in the route:

```
RP/0/RP0/CPU0:router(config-rpl)# if rib-has-route pf1 then
```

R3.3 Beta Draft—Cisco Confidential Information

route-policy (RPL)

To define a route policy and enter route-policy configuration mode, use the **route-policy** command in global configuration mode. To remove a policy definition, use the **no** form of this command.

route-policy *name*

no route-policy *name*

Syntax Description

<i>name</i>	Name of a route policy.

Defaults

No default behavior or value

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **route-policy** command to define a route policy and enter route-policy configuration mode.

Policy definitions create named bundles of policy statements. A policy definition consists of the **route-policy** command followed by a name, a group of policy statements, and the **end-policy** command.

The policy name serves as a handle for binding the policy to protocols.

Task ID

Task ID	Operations
route-policy	read, write

Examples

The following example shows a simple policy named drop-everything that drops any route it encounters:

```
RP/0/RP0/CPU0:router(config)# route-policy drop-everything
RP/0/RP0/CPU0:router(config-rpl)# drop
RP/0/RP0/CPU0:router(config-rpl)# end-policy
```

R3.3 Beta Draft—Cisco Confidential Information

Policies may also refer to other policies such that common blocks of policy can be reused. This reference to other policies is accomplished by using the **apply** command. The following is a simple example:

```
RP/0/RP0/CPU0:router(config)# route-policy drop-as-1234
RP/0/RP0/CPU0:router(config-rpl)# if as-path passes-through '1234' then
RP/0/RP0/CPU0:router(config-rpl-if)# apply check-communities
RP/0/RP0/CPU0:router(config-rpl-if)# else
RP/0/RP0/CPU0:router(config-rpl-if)# pass
RP/0/RP0/CPU0:router(config-rpl-if)# endif
RP/0/RP0/CPU0:router(config-rpl-if)# end-policy
```

The **apply** command indicates that the policy check-communities should be executed if the route under consideration passed through autonomous system 1234 before it was received. If so, the communities of the route are checked, and based on the findings the route may be accepted unmodified, accepted with changes, or dropped.

Related Commands

Command	Description
end-policy	Ends the definition of a route policy.

R3.3 Beta Draft—Cisco Confidential Information

route-type is

To match route types when redistribution is being performed into Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), or Integrated Intermediate System-to-Intermediate System (IS-IS), use the **route-type is** command in route-policy configuration mode.

route-type is {**local** | **interarea** | **internal** | **type-1** | **type-2** | **level-1** | **level-2** | **level-1-2** | *parameter*}

Syntax Description		
local		Uses a local value to match locally generated OSPF routes.
interarea		Uses an interarea value to match IS-IS interarea routes.
internal		Uses an internal value to match OSPF intra- and interarea routes.
type-1		Uses a Type 1 value to match Type 1 OSPF routes.
type-2		Uses a Type 2 value to match Type 2 OSPF routes.
level-1		Uses a Level 1 value to match Level 1 IS-IS routes.
level-2		Uses a Level 2 value to match Level 2 IS-IS routes.
level-1-2		Uses an interarea value to match IS-IS interarea routes.
<i>parameter</i>		Parameterized value that fills one of the required values.

Defaults No default behavior or value

Command Modes Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. he level-1-2 keyword was replaced with the interarea keyword.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **route-type is** command as a conditional expression within an **if** statement to compare route types when redistribution is being performed into BGP, OSPF, or IS-IS.

**Note**

For a list of all conditional expressions available within an **if** statement, see the **if** command.

R3.3 Beta Draft—Cisco Confidential Information

The valid keywords are **local**, **internal**, **type-1**, **type-2**, **level-1**, **level-2**, and **level-1-2**. A parameterized value that fills in one of these values may also be used. The **local** value is used to match locally generated BGP routes. The **internal** value is used to match OSPF intra- and interarea routes. The **type-1** and **type-2** values are used to match Type 1 and Type 2 OSPF external routes. The **level-1**, **level-2**, and **level-1-2** values are used to match IS-IS routes of those respective types.

Because the route type is a matching operator, it appears in conditional clauses of **if** and **then** statements.

Task ID

Task ID	Operations
route-policy	read, write

Examples

In the following example, if the route type is local then an action or a sequence of operations that modify a route, most of which are distinguished by the **set** keyword, takes place:

```
RP/0/RP0/CPU0:router(config)# route-policy policy_A
RP/0/RP0/CPU0:router(config-rpl)# if route-type is local then
```


R3.3 Beta Draft—Cisco Confidential Information

rpl maximum

To configure the number of lines of configuration limit and the number of policies limit, use the **rpl maximum** command in global configuration mode.

rpl maximum {*lines number* | *policies number*}

Syntax Description	lines <i>number</i>	Configures the number of lines of configuration limit. Range is 1 to 131072.
	policies <i>number</i>	Configures the number of policies limit. Range is 1 to 5000.

Defaults	<i>lines</i> : 65536 <i>policies</i> : 3500

Command Modes	Global configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **rpl maximum** command to configure system limits on the routing policy subsystem. As such, **rpl maximum** configuration lines do not appear as statements within a routing policy. This command places resource limits on the routing policy subsystem. Use the **rpl maximum** command to configure the maximum number of lines of configuration and number of policies.

The number of lines of configuration includes the beginning and ending statements, for example, **route-policy** and **end-policy**. Each line of configuration for sets is also counted.

A line of configuration is counted only once; it is not counted each time it is used. Similarly, any multiple use of policy in an apply statement counts only as one policy.

A user can change the default values for lines and policies but cannot exceed the maximum value, nor can the value for lines and policies be configured lower than the number of lines or policies that are currently configured.

Task ID	Task ID	Operations
	route-policy	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

In the following example, the maximum number of configuration lines is set to 50 and the maximum number of policies is set to 6:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rpl maximum lines 50
RP/0/RP0/CPU0:router(config)# rpl maximum policies 6
```

Related Commands

Command	Description
show rpl maximum	Displays the maximum limits for lines of configuration and number of policies.

R3.3 Beta Draft—Cisco Confidential Information

set community

To set the Border Gateway Protocol (BGP) community attribute, use the **set community** command in route-policy configuration mode.

set community { *community-set-name* | *inline-community-set* } [**additive**]

Syntax Description

<i>community-set-name</i>	Community set name.
<i>inline-community-set</i>	Inline community set.
additive	(Optional) Adds communities to communities in the route.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **set community** command to set the BGP community attribute.



Note

The **set community** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

Communities are 32-bit values carried in BGP routes. Each route may have zero or more communities in an unordered list.

Use this command to replace the communities in a route or add to them using the optional **additive** keyword.

As with the other community forms that support inline sets, either or both 16-bit portions of the community can be parameterized. Likewise, the names of the well-known communities internet, no-advertise, no-export, and local-AS can also be used.

Without the **additive** keyword, any existing communities (other than the well-known communities) are removed and replaced with the given communities. The **additive** keyword specifies that all communities already present in the route be maintained and the list of communities be added to them.

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	route-policy	read, write

Examples

The following are incomplete configuration examples using the **set community** command:

```

RP/0/RP0/CPU0:router(config-rpl)# set community (10:24)
RP/0/RP0/CPU0:router(config-rpl)# set community (10:24, $as:24, $as:$tag)
RP/0/RP0/CPU0:router(config-rpl)# set community (10:24, internet) additive
RP/0/RP0/CPU0:router(config-rpl)# set community (10:24, $as:24) additive

```

R3.3 Beta Draft—Cisco Confidential Information

set cost

To set the cost attribute for routes that are redistributed into Open Shortest Path First (OSPF), use the **set cost** command in route-policy configuration mode.

```
set cost {integer | parameter}
```

Syntax Description

<i>integer</i>	Cost attribute for the route specified as an integer value.
<i>parameter</i>	Cost attribute for the route specified as a parameter value.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **set cost** command to set the cost attribute for routes that are redistributed into OSPF.

**Note**

The **set cost** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

This command takes either an integer or a parameter value as an argument.

Task ID

Task ID	Operations
route-policy	read, write

Examples

In the following example, the OSPF cost attribute is set to 10:

```
RP/0/RP0/CPU0:router(config-rpl)# set cost 10
```

In this example, the cost attribute is set to the parameter value \$ospf_cost:

```
RP/0/RP0/CPU0:router(config-rpl)# set cost $ospf_cost
```

R3.3 Beta Draft—Cisco Confidential Information

set dampening

To configure Border Gateway Protocol (BGP) route dampening, use the **set dampening** command in route-policy configuration mode.

set dampening {**halflife** *minutes* | **max-suppress** *minutes* | **reuse** *seconds* | **suppress** *penalty-units* }
others default

Syntax Description		
	halflife <i>minutes</i>	Specifies the time (in minutes) after which a penalty is decreased. After the route 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. Range is 1 to 45 minutes.
	max-suppress <i>minutes</i>	Specifies the maximum time (in minutes) a route can be suppressed. Range is 1 to 20000. If the half-life value is allowed to default, the maximum suppress time defaults to 60 minutes.
	reuse <i>seconds</i>	Unsuppresses a route if the penalty for flapping the route decreases enough to fall below the configured value (in seconds). The process of unsuppressing routes occurs at 10-second increments. Range is 1 to 20000.
	suppress <i>penalty-units</i>	Specifies a penalty of 1000 each time a route flaps. When a route penalty exceeds the configured limit, it is suppressed. Range is 1 to 20000.
	others default	Specifies that the command <i>must</i> end with others default , which indicates that any keyword not defined is set to its default.

Defaults	
	half-life: 15 minutes
	max-suppress: 60 minutes (four times the half-life)
	reuse: 750 seconds
	suppress: 2000 penalty units

Command Modes	
	Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	
	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

The BGP protocol supports route dampening using an exponential backoff algorithm. The algorithm is controlled by setting the four supported BGP values: half-life, max-suppress, reuse, and suppress. Use the **set dampening** command to configure BGP route dampening.

R3.3 Beta Draft – Cisco Confidential Information

**Note**

The **set dampening** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

A value for at least one of the four keywords must be set. If the **set dampening** command defines values for three or fewer of the supported keywords, then the configuration must end with the **others default**, which indicates that any keyword value not defined in the command is set to its default value.

The keywords may appear in the command in any order.

Task ID

Task ID	Operations

route-policy	read, write

Examples

In the following examples, half-life is set to 20 minutes and the maximum suppress time is set to 90 minutes. Each command must end with **others default** because three or fewer keywords are defined.

```
RP/0/RP0/CPU0:router(config-rpl)# set dampening halflife 20 others default
RP/0/RP0/CPU0:router(config-rpl)# set dampening max-suppress 90 others default
```

In this example, all four keywords are defined, which means the command does not use **others default**.

```
RP/0/RP0/CPU0:router(config-rpl)# set dampening halflife 15 max-suppress 60 reuse 750
suppress 2000
```

The following command is invalid because it is missing **others default**.

```
RP/0/RP0/CPU0:router(config-rpl)# set dampening reuse 700
```

R3.3 Beta Draft—Cisco Confidential Information

set eigrp-metric

To set Enhanced Interior Gateway Routing Protocol (EIGRP) metric attributes, use the set eigrp-metric command in route-policy configuration mode.

set eigrp-metric *bandwidth delay reliability loading mtu*

Syntax Description		
<i>bandwidth</i>		Minimum bandwidth of the route in kilobits per second. Range is 1 to 4294967295.
<i>delay</i>		Route delay in tens of microseconds. Delay is 1 or any positive number that is a multiple of 39.1 nanoseconds. Range is 1 to 4294967295.
<i>reliability</i>		Likelihood of successful packet transmission expressed as a number between 0 and 255. The value 255 means 100 percent reliability; 0 means no reliability.
<i>loading</i>		Effective bandwidth of the route expressed as a number from 1 to 255 (255 is 100 percent loading).
<i>mtu</i>		Minimum maximum transmission unit (MTU) size of the route in bytes. Range is from 1 to 65535.

Defaults	None

Command Modes	Route-policy configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. You can use the add command to further offset an existing EIGRP metric value.

Task ID	Task ID	Operations
	route-policy	read, write

Examples	In the following example, the EIGRP metrics are adjusted for route policy policy_1: <pre>RP/0/RP0/CPU0:router(config)# route-policy policy_1 RP/0/RP0/CPU0:router(config-rpl)# set eigrp-metric 1400 120 250 100 1500</pre>

R3.3 Beta Draft—Cisco Confidential Information

Related Commands	Command	Description
	add	Adds an offset to an existing value.

R3.3 Beta Draft—Cisco Confidential Information

set extcommunity

To set the Border Gateway Protocol (BGP) extended community attribute, use the **set extcommunity** command in route-policy configuration mode.

set extcommunity {*extcommunity-set-name* | *inline-extcommunity-set*} [**additive**]

Syntax Description

<i>extcommunity-set-name</i>	Extended community set name.
<i>inline-extcommunity-set</i>	Inline extended community set.
additive	(Optional) Adds extended communities to extended communities in the route.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **set extcommunity** command to either replace the extended communities on the route or add to them using the optional **additive** keyword.

**Note**

The **set extcommunity** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

As with the other extended community forms that support inline sets, either or both portions of the community can be parameterized. Similarly to regular communities, the **additive** keyword can be used to signify adding these extended communities to those that are already present, as opposed to replacing them.

Task ID

Task ID	Operations
route-policy	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

The following are incomplete configuration examples using the **set extcommunity** command:

```
RP/0/RP0/CPU0:router(config-rpl)# set extcommunity (10:24)
RP/0/RP0/CPU0:router(config-rpl)# set extcommunity (10:24, $as:24, $as:$tag)
RP/0/RP0/CPU0:router(config-rpl)# set extcommunity (10:24, internet) additive
RP/0/RP0/CPU0:router(config-rpl)# set extcommunity (10:24, $as:24) additive
```

Without the **additive** keyword, any existing extended communities (other than the well-known communities) are removed and replaced with the given communities. The **additive** keyword specifies that all extended communities already present in the route be maintained and the list of extended communities be added to them.

R3.3 Beta Draft—Cisco Confidential Information

set level

To configure the integrated Intermediate System-to-Intermediate System (IS-IS) level in which redistributed routes should be sent, use the **set level** command in route-policy configuration mode.

set level {**level-1** | **level-2** | **level-1-2** | *parameter*}

Syntax Description

level-1	Uses Level 1 to match Level 1 IS-IS routes.
level-2	Uses Level 2 to match Level 2 IS-IS routes.
level-1-2	Uses Level 1-2 to match either Level 1 or Level 2 IS-IS routes.
<i>parameter</i>	Parameter value.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the IS-IS **set level** command to configure the IS-IS level in which redistributed routes should be sent.

**Note**

The **set level** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

This command supports parameterization of the **level** keyword.

Task ID

Task ID	Operations
route-policy	read, write

Examples

In the following example, the level is set to Level 1:

```
RP/0/RP0/CPU0:router(config-rpl)# set level level-1
```

R3.3 Beta Draft—Cisco Confidential Information

set local-preference

To assign a value to a 32-bit unsigned integer, use the **set local-preference** command in route-policy configuration mode.

set local-preference { *integer* | *parameter* }

Syntax Description	<i>integer</i>	Value assigned to a 32-bit unsigned integer . Range is 0 to 4294967295.
	<i>parameter</i>	Parameter value assigned to a 32-bit unsigned integer.

Defaults Default value is 100.

Command Modes Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **set local-preference** command to specify a preference value for the autonomous system path. Local preference is a nontransitive (does not cross autonomous system boundaries) attribute and is the second metric considered in the BGP best path calculation (the highest local preference is chosen). Weight is the first metric evaluated for best path, but it is local to the router and propagates only to iBGP peers. See the *Implementing BGP on Cisco IOS XR Software* module of the *Cisco IOS XR Routing Configuration Guide* for information on the BGP best path calculation.



Note

The **set local-preference** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

The local preference is a 32-bit unsigned integer.

Task ID	Task ID	Operations
	route-policy	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

In the following example, the local preference value is set to 10:

```
RP/0/RP0/CPU0:router(config-rpl)# set local-preference 10
```

R3.3 Beta Draft—Cisco Confidential Information**set med**

To set the Border Gateway Protocol (BGP) Multi Exit Discriminator (MED) attribute, use the **set med** command in route-policy configuration mode.

set med { *integer* | *parameter* | **igp-cost** | { + | - } { *integer* | *parameter* } | **max-reachable** }

Syntax Description	<i>integer</i>	32-bit number. Range is 0 to 4294967295.
	<i>parameter</i>	Parameter value.
	igp-cost	Sets the MED value to the cost for the Interior Gateway Protocol (IGP) route to resolve the next hop of the BGP route.
	+ -	Sets the MED to the MED plus or minus a static offset. An integer or parameter must follow the plus or minus.
	max-reachable	Sets the MED value to the maximum possible value.

Defaults No default behavior or value

Command Modes Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **set med** command to set the MED value, which is a 32-bit unsigned integer.

**Note**

The **set med** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

This command can take the following as argument values: an integer, a parameter, the **igp-cost** keyword, or a mathematical operator (either plus or minus) followed by an integer or a parameter.

The plus or minus variants allow the user to set the MED to the MED plus or minus a static offset. The variants that allow a user to add or subtract offsets to the MED value are also range checked for underflow or overflow. If the value underflows as a result of subtraction, then the MED value is set to zero. If the value overflows, the value is set to 4294967295, which is a special value for MED.

R3.3 Beta Draft – Cisco Confidential Information

Task ID	Task ID	Operations
	route-policy	read, write

Examples The following two examples show how to set the MED to a value that is either specified directly (using the integer 156) or passed to the policy as a parameter:

```
RP/0/RP0/CPU0:router(config-rpl)# set med 156
RP/0/RP0/CPU0:router(config-rpl)# set med $med_param
```

The following example shows how to instruct BGP to automatically set the MED value to the cost of the IGP route that resolves the next hop of the BGP route:

```
RP/0/RP0/CPU0:router(config-rpl)# set med igp-cost
```


R3.3 Beta Draft—Cisco Confidential Information

set metric

To configure the link metric of routes that are redistributed into integrated Intermediate System-to-Intermediate System (IS-IS), use the **set metric** command in route-policy configuration mode.

set metric { *integer* | *parameter* }

Syntax Description	<i>integer</i>	Integer value assigned to the link of metric routes . Range is 0 to 1677215.
	<i>parameter</i>	Parameter value assigned to the link of metric routes.

Defaults	No default behavior or value

Command Modes	Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **set metric** command to configure the link metric of routes that are redistributed into IS-IS.

**Note**

The **set metric** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

The metric attribute is used by IS-IS to calculate the cost of the route. IS-IS supports both narrow link metrics from 0 to 63 and wide link metrics from 0 to 16777215.

This command also supports a parameter value.

Task ID	Task ID	Operations
	route-policy	read, write

Examples	In the following example, the metric attribute is set to 10:

```
RP/0/RP0/CPU0:router(config-rpl)# set metric 10
```

R3.3 Beta Draft—Cisco Confidential Information

set metric-type (IS-IS)

To configure the integrated Intermediate System-to-Intermediate System (IS-IS) metric type, use the **set metric-type** command in route-policy configuration mode.

set metric-type { **internal** | **external** | *parameter* }

Syntax Description

internal	Sets metric type to internal.
external	Sets the metric type to external.
<i>parameter</i>	Specific parameter for the metric type.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the IS-IS **set metric-type** command to control whether IS-IS treats the metric as an internal or external metric.

**Note**

The **set metric-type** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

This command does not support parameterization.

Task ID

Task ID	Operations
route-policy	read, write

Examples

In the following example, the IS-IS metric type is set to internal:

```
RP/0/RP0/CPU0:router(config-rpl)# set metric-type internal
```

R3.3 Beta Draft—Cisco Confidential Information

set metric-type (OSPF)

To control how Open Shortest Path First (OSPF) computes the cost for a route, use the **set metric-type** command in route-policy configuration mode.

set metric-type {type-1 | type-2}

Syntax Description	type-1	Uses the cost set on the route plus the topology-related costs in the calculation for Type 1 metrics.
	type-2	Uses only the cost set on the route in the calculation for Type 2 metrics.

Defaults No default behavior or value

Command Modes Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the OSPF **set metric-type** command to control whether OSPF treats the cost as a Type 1 or Type 2 metric.



Note

The **set metric-type** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

The value of Type 1 or Type 2 controls how OSPF computes the cost for this route. For Type 2 metrics, only the cost set on the route is used. For Type 1 metrics, the cost set on the route plus the topology-related costs are used in the calculation.

This command does not support parameterization.

Task ID	Task ID	Operations
	route-policy	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

In the following example, the OSPF metric type is set to Type 1:

```
RP/0/RP0/CPU0:router(config-rpl)# set metric-type type-1
```

R3.3 Beta Draft—Cisco Confidential Information

set next-hop

To replace the next hop associated with a given route, use the **set next-hop** command in route-policy configuration mode.

set next-hop {*ipv4-address* | *ipv6-address* | **peer-address** | *parameter*}

Syntax Description

<i>ipv4-address</i>	Valid IPv4 address.
<i>ipv6-address</i>	Valid IPv6 address.
peer-address	Sets the next hop to the IP address of the remote Border Gateway Protocol (BGP) peer.
<i>parameter</i>	Parameter value.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **set next-hop** command to replace the next hop associated with a given route.



Note

The **set next-hop** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

Use the **set next-hop peer-address** command to set the next hop to the address of the BGP neighbor, where this policy is attached.

The next hop is a valid IPv4 address entered as a dotted decimal or an IPv6 address entered as a colon-separated hexadecimal.

It is not possible to use this command to set the BGP IPv6 link-local next hop.

Task ID

Task ID	Operations
route-policy	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

In the following example, the next hop is set to a valid IPv4 address:

```
RP/0/RP0/CPU0:router(config-rpl)# set next-hop 10.0.0.5
```

In this example, the next hop is set to a parameter value \$nexthop:

```
RP/0/RP0/CPU0:router(config-rpl)# set next-hop $nexthop
```

R3.3 Beta Draft—Cisco Confidential Information

set origin

To change the origin attribute, use the **set origin** command in route-policy configuration mode.

```
set origin {igp | incomplete | egp | parameter}
```

Syntax Description	igp	Sets the origin type to Interior Gateway Protocol (IGP).
	incomplete	Sets the origin type to incomplete.
	egp	Sets the origin type to Exterior Gateway Protocol (EGP).
	<i>parameter</i>	Specific parameter for the origin type.

Defaults	No default behavior or values

Command Modes	Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **set origin** command to change the origin attribute.



Note	The set origin command can be used as an action statement within an if statement. For a list of all action statements available within an if statement, see the if command.

The origin of a Border Gateway Protocol (BGP) route is **igp**, **egp**, or **incomplete**.

Task ID	Task ID	Operations
	route-policy	read, write

Examples	In the following example, the origin attribute is set to EGP:

```
RP/0/RP0/CPU0:router(config-rpl)# set origin egp
```

R3.3 Beta Draft—Cisco Confidential Information

set rip-metric

To set Routing Information Protocol (RIP) metric attributes, use the **set rip-metric** command in route-policy configuration mode.

set rip-metric [*number* | *parameter*]

Syntax Description

<i>number</i>	Four bit decimal number. Range is from 0 to 16.
<i>parameter</i>	Bandwidth in kilobits per second. Range is from 0 to 4294967295.

Defaults**Command Modes**

Route-policy configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

You can use the **add** command to further offset an existing RIP metric value.

Task ID

Task ID	Operations
route-policy	read, write

Examples

In the following example, the RIP metric number is adjusted for route policy policy_1:

```
RP/0/RP0/CPU0:router(config)# route-policy policy_1
RP/0/RP0/CPU0:router(config-rpl)# set rip-metric 10
```

Related Commands

Command	Description
add	Adds an offset to an existing value.

R3.3 Beta Draft – Cisco Confidential Information

set tag

To set the tag attribute, use the **set tag** command in route-policy configuration mode.

```
set tag {integer | parameter}
```

Syntax Description	<i>integer</i>	Integer value assigned to the tag attribute. Value is from 0 to 4294967295.
	<i>parameter</i>	Parameter value assigned to the tag attribute.

Defaults	No default behavior or value

Command Modes	Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

Use the **set tag** command to set the tag attribute.

**Note**

The **set tag** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

Tags are 32-bit integers that can be associated with a given route.

For the Border Gateway Protocol (BGP), the tag attribute can be set only at the table-policy attach point.

Task ID	Task ID	Operations
	route-policy	read, write

Examples	In the following example, the tag attribute is set to 10: <pre>RP/0/RP0/CPU0:router(config-rpl)# set tag 10</pre>
	In this example, the tag attribute is set to a parameter value \$tag_param: <pre>RP/0/RP0/CPU0:router(config-rpl)# set tag \$tag_param</pre>

R3.3 Beta Draft—Cisco Confidential Information

set traffic-index

To set the traffic index attribute, use the **set traffic-index** command in route-policy configuration mode.

set traffic-index {*integer* | *parameter* | **ignore**}

Syntax Description	<i>integer</i>	Integer value assigned to the traffic index attribute. Range is 1 to 63.
	<i>parameter</i>	Parameter value assigned to the traffic index attribute.
	ignore	Specifies that Border Gateway Protocol (BGP) policy accounting is not done.

Defaults	No default behavior or value

Command Modes	Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **set traffic-index** command to set the traffic index attribute.

**Note**

The **set traffic-index** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

Traffic index is a special attribute for BGP. It is used as an index to a set of counters that are maintained by forwarding hardware. It is also used to track packet and byte counters that are forwarded using routes with specific attributes. These counters can be enabled and disabled on an individual interface basis.

The traffic index attribute can be set only at the table-policy attach point, and can take a value from 1 to 63, or a value of **ignore**. If the traffic index is set to **ignore**, then BGP policy accounting is not done. Parameterization of this value is also supported.

Task ID	Task ID	Operations
	route-policy	read, write

R3.3 Beta Draft—Cisco Confidential Information

Examples

In the following example, a policy is created in which the traffic index is set to 10 for all routes that originated in autonomous system 1234:

```
RP/0/RP0/CPU0:router(config)# route-policy count-as-1234
RP/0/RP0/CPU0:router(config-rpl)# if as-path originates-from '1234' then
RP/0/RP0/CPU0:router(config-rpl-if)# set traffic-index 10
RP/0/RP0/CPU0:router(config-rpl-if)# else
RP/0/RP0/CPU0:router(config-rpl-if)# pass
RP/0/RP0/CPU0:router(config-rpl-if)# endif
RP/0/RP0/CPU0:router(config-rpl-if)# end-policy
```

This policy could then be attached using the BGP **table-policy** command. The counters could then be enabled on various interfaces with the appropriate commands.

R3.3 Beta Draft—Cisco Confidential Information

set weight

To set the weight value for Border Gateway Protocol (BGP) routes, use the **set weight** command in route-policy configuration mode.

set weight {*number* | *parameter*}

Syntax Description

<i>number</i>	Number assigned to the weight value for BGP routes. Weight is 16 bits. Range is 0 to 65535.
<i>parameter</i>	Parameter assigned to the weight value for BGP routes.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **set weight** command to set the weight value for BGP routes.

**Note**

The **set weight** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

The weight of a route is a value attached to the route for use in route selection. It is used to establish a precedence between different routing protocols when they both want to install routes to the same destination network.

Given two BGP routes with the same network layer reachability index (NLRI), a route with a higher weight is selected, no matter what the values of other BGP attributes may be. However, weight only has significance on the local router. It is not sent from one BGP speaker to another, even within the same autonomous system.

On Cisco routers, if a route is sourced by the local router, its weight is automatically set to 32768; if the route is learned from another router, its weight is automatically set to 0. Thus, by default, locally sourced routes are preferred over learned routes.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	route-policy	read, write

Examples

In the following examples, the weight of the route is set to 10 and then to a parameter value \$weight_param:

```
RP/0/RP0/CPU0:router(config-rpl)# set weight 10
RP/0/RP0/CPU0:router(config-rpl)# set weight $weight_param
```

R3.3 Beta Draft—Cisco Confidential Information

show rpl active as-path-set

To display the AS path sets that are referenced by at least one policy that is being used at an attach point, use the **show rpl active as-path-set** command in EXEC mode.

show rpl active as-path-set

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **show rpl active as-path-set** command to display all AS path sets that are in use in the system and referenced either directly or indirectly at a policy attach point.

Task ID	Task ID	Operations
	route-policy	read

Examples	This example shows the following sample configuration:

```
router bgp 2
  address-family ipv4 unicast
  !
  neighbor 10.0.101.2
    remote-as 100
    address-family ipv4 unicast
    route-policy policy_1 in
  !
  neighbor 10.0.101.3
    remote-as 12
    address-family ipv4 unicast
    route-policy policy_2 in
```

R3.3 Beta Draft—Cisco Confidential Information

```

!
!
!
RP/0/RP0/CPU0:router# show rpl route-policy policy_2 detail

prefix-set prefix_set_ex1
  10.0.0.0/16 ge 16 le 32,
  0.0.0.0/0 ge 25 le 32,
  0.0.0.0/0
end-set
!
community-set comm_set_ex1
  65500:1,
  65500:2,
  65500:3
end-set
!
extcommunity-set ext_comm_set_ex1
  S00:65500:1,
  RT:1.2.3.4:34
end-set
!
route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy
!

RP/0/RP0/CPU0:router# show rpl route-policy policy_1 detail

prefix-set prefix_set_ex1
  10.0.0.0/16 ge 16 le 32,
  0.0.0.0/0 ge 25 le 32,
  0.0.0.0/0
end-set
!
as-path-set as_path_set_ex1
  ios-regex '^_655--$',
  ios-regex '^_65501_$'
end-set
!
route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!

```

Given this sample configuration, the **show rpl active as-path-set** command displays the following information:

```
RP/0/RP0/CPU0:router# show rpl active as-path-set
```

```
ACTIVE -- Referenced by at least one policy which is attached
INACTIVE -- Only referenced by policies which are not attached
```

■ **show rpl active as-path-set**

R3.3 Beta Draft – Cisco Confidential Information

UNUSED -- Not attached (directly or indirectly) and not referenced

The following as-path-sets are ACTIVE

as_path_set_ex1

Related Commands	Command	Description
	show rpl active community-set	Displays the community sets that are referenced by at least one policy that is being used at an attach point.
	show rpl active extcommunity-set	Displays the extended community sets that are referenced by at least one policy that is being used at an attach point.
	show rpl active route-policy	Displays the route policies that are referenced by at least one policy that is being used at an attach point.
	show rpl active prefix-set	Displays the prefix sets that are referenced by at least one policy that is being used at an attach point.

R3.3 Beta Draft – Cisco Confidential Information

show rpl active community-set

To display the community sets that are referenced by at least one policy that is being used at an attach point, use the **show rpl active community-set** command in EXEC mode.

show rpl active community-set

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or value

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show rpl active community-set** command to display all community sets that are in use in the system and referenced either directly or indirectly at a policy attach point.

Task ID	Task ID	Operations
	route-policy	read

Examples This example shows the following sample configuration:

```
router bgp 2
 address-family ipv4 unicast
 !
 neighbor 10.0.101.2
  remote-as 100
  address-family ipv4 unicast
   route-policy policy_1 in
 !
 !
 neighbor 10.0.101.3
  remote-as 12
  address-family ipv4 unicast
   route-policy policy_2 in
```

R3.3 Beta Draft—Cisco Confidential Information

```

!
!
!

RP/0/RP0/CPU0:router# show rpl route-policy policy_2 detail

prefix-set prefix_set_ex1
  10.0.0.0/16 ge 16 le 32,
  0.0.0.0/0 ge 25 le 32,
  0.0.0.0/0
end-set
!
community-set comm_set_ex1
  65500:1,
  65500:2,
  65500:3
end-set
!
extcommunity-set ext_comm_set_ex1
  SOO:65500:1,
  RT:1.2.3.4:34
end-set
!
route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy
!

RP/0/RP0/CPU0:router# show rpl route-policy policy_1 detail

prefix-set prefix_set_ex1
  10.0.0.0/16 ge 16 le 32,
  0.0.0.0/0 ge 25 le 32,
  0.0.0.0/0
end-set
!
as-path-set as_path_set_ex1
  ios-regex '^_655--$',
  ios-regex '^_65501_$'
end-set
!
route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!
```

Given this sample configuration, the **show rpl active community-set** command displays the following information:

```

RP/0/RP0/CPU0:router# show rpl active community-set

ACTIVE -- Referenced by at least one policy which is attached
```

R3.3 Beta Draft – Cisco Confidential Information

INACTIVE -- Only referenced by policies which are not attached
 UNUSED -- Not attached (directly or indirectly) and not referenced

The following community-sets are ACTIVE

 comm_set_ex1

Related Commands

Command	Description
show rpl active as-path-set	Displays the AS path sets that are referenced by at least one policy that is being used at an attach point.
show rpl active extcommunity-set	Displays the extended community sets that are referenced by at least one policy that is being used at an attach point.
show rpl active route-policy	Displays the route policies that are referenced by at least one policy that is being used at an attach point.
show rpl active prefix-set	Displays the prefix sets that are referenced by at least one policy that is being used at an attach point.

R3.3 Beta Draft—Cisco Confidential Information

show rpl active extcommunity-set

To display the extended community sets that are referenced by at least one policy that is being used at an attach point, use the **show rpl active extcommunity-set** command in EXEC mode.

show rpl active extcommunity-set

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **show rpl active extcommunity-set** command to display all extended community sets that are in use in the system and referenced either directly or indirectly at a policy attach point.

Task ID	Task ID	Operations
	route-policy	read

Examples	This example shows the following sample configuration:

```
router bgp 2
  address-family ipv4 unicast
  !
  neighbor 10.0.101.2
    remote-as 100
    address-family ipv4 unicast
    route-policy policy_1 in
  !
  !
  neighbor 10.0.101.3
    remote-as 12
    address-family ipv4 unicast
    route-policy policy_2 in
```

R3.3 Beta Draft—Cisco Confidential Information

```

!
!
!

RP/0/RP0/CPU0:router# show rpl route-policy policy_2 detail

prefix-set prefix_set_ex1
  10.0.0.0/16 ge 16 le 32,
  0.0.0.0/0 ge 25 le 32,
  0.0.0.0/0
end-set
!
community-set comm_set_ex1
  65500:1,
  65500:2,
  65500:3
end-set
!
extcommunity-set ext_comm_set_ex1
  S00:65500:1,
  RT:1.2.3.4:34
end-set
!
route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy
!

RP/0/RP0/CPU0:router# show rpl route-policy policy_1 detail

prefix-set prefix_set_ex1
  10.0.0.0/16 ge 16 le 32,
  0.0.0.0/0 ge 25 le 32,
  0.0.0.0/0
end-set
!
as-path-set as_path_set_ex1
  ios-regex '^_655--$',
  ios-regex '^_65501_$'
end-set
!
route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!

```

Given this sample configuration, the **show rpl active extcommunity-set** command displays the following information:

```

RP/0/RP0/CPU0:router# show rpl active extcommunity-set

ACTIVE -- Referenced by at least one policy which is attached

```

■ **show rpl active extcommunity-set**

R3.3 Beta Draft – Cisco Confidential Information

INACTIVE -- Only referenced by policies which are not attached

UNUSED -- Not attached (directly or indirectly) and not referenced

The following extcommunity-sets are ACTIVE

ext_comm_set_ex1

Related Commands

Command	Description
show rpl active as-path-set	Displays the AS path sets that are referenced by at least one policy that is being used at an attach point.
show rpl active community-set	Displays the community sets that are referenced by at least one policy that is being used at an attach point.
show rpl active route-policy	Displays the route policies that are referenced by at least one policy that is being used at an attach point.
show rpl active prefix-set	Displays the prefix sets that are referenced by at least one policy that is being used at an attach point.

R3.3 Beta Draft—Cisco Confidential Information

show rpl active route-policy

To display the route policies that are referenced by at least one policy that is being used at an attach point, use the **show rpl active route-policy** command in EXEC mode.

show rpl active route-policy

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The policy keyword was changed to route-policy .
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **show rpl active route-policy** command to display all policies that are in use in the system and referenced either directly or indirectly at a policy attach point.

Task ID	Task ID	Operations
	route-policy	read

Examples	This example shows the following sample configuration:

```
router bgp 2
  address-family ipv4 unicast
  !
  neighbor 10.0.101.2
    remote-as 100
    address-family ipv4 unicast
      route-policy policy_1 in
    !
  !
  neighbor 10.0.101.3
    remote-as 12
```

R3.3 Beta Draft—Cisco Confidential Information

```

address-family ipv4 unicast
  route-policy policy_2 in
!
!
!

RP/0/RP0/CPU0:router# show rpl route-policy policy_1

route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!
RP/0/RP0/CPU0:router# show rpl route-policy policy_2

route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy
!
```

Given this sample configuration, the **show rpl active route-policy** command displays the following information:

```

RP/0/RP0/CPU0:router# show rpl active route-policy

ACTIVE -- Referenced by at least one policy which is attached
INACTIVE -- Only referenced by policies which are not attached
UNUSED -- Not attached (directly or indirectly) and not referenced

The following policies are (ACTIVE)
-----
policy_1
policy_2
```

Related Commands

Command	Description
show rpl active as-path-set	Displays the AS path sets that are referenced by at least one policy that is being used at an attach point.
show rpl active community-set	Displays the community sets that are referenced by at least one policy that is being used at an attach point.
show rpl active extcommunity-set	Displays the extended community sets that are referenced by at least one policy that is being used at an attach point.
show rpl active prefix-set	Displays the prefix sets that are referenced by at least one policy that is being used at an attach point.

R3.3 Beta Draft – Cisco Confidential Information

show rpl active prefix-set

To display the prefix sets that are referenced by at least one policy that is being used at an attach point, use the **show rpl active prefix-set** command in EXEC mode.

show rpl active prefix-set

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or value

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show rpl active prefix-set** command to display all prefix sets that are in use in the system and referenced either directly or indirectly at a policy attach point.

Task ID	Task ID	Operations
	route-policy	read

Examples This example shows the following sample configuration:

```
router bgp 2
 address-family ipv4 unicast
 !
 neighbor 10.0.101.2
  remote-as 100
  address-family ipv4 unicast
   route-policy policy_1 in
 !
 !
 neighbor 10.0.101.3
  remote-as 12
  address-family ipv4 unicast
   route-policy policy_2 in
```

R3.3 Beta Draft—Cisco Confidential Information

```

!
!
!

RP/0/RP0/CPU0:router# show rpl route-policy policy_2 detail

prefix-set prefix_set_ex1
  10.0.0.0/16 ge 16 le 32,
  0.0.0.0/0 ge 25 le 32,
  0.0.0.0/0
end-set
!

community-set comm_set_ex1
  65500:1,
  65500:2,
  65500:3
end-set
!

extcommunity-set ext_comm_set_ex1
  SOO:65500:1,
  RT:1.2.3.4:34
end-set
!

route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy
!

RP/0/RP0/CPU0:router# show rpl route-policy policy_1 detail

prefix-set prefix_set_ex1
  10.0.0.0/16 ge 16 le 32,
  0.0.0.0/0 ge 25 le 32,
  0.0.0.0/0
end-set
!

as-path-set as_path_set_ex1
  ios-regex '^_655--$',
  ios-regex '^_65501_$'
end-set
!

route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!

```

The following example displays active prefix sets:

```
RP/0/RP0/CPU0:router# show rpl active prefix-set
```

```
ACTIVE -- Referenced by at least one policy which is attached
```

R3.3 Beta Draft – Cisco Confidential Information

INACTIVE -- Only referenced by policies which are not attached
 UNUSED -- Not attached (directly or indirectly) and not referenced

The following prefix-sets are ACTIVE

 prefix_set_1

Related Commands

Command	Description
show rpl active as-path-set	Displays the AS path sets that are referenced by at least one policy that is being used at an attach point.
show rpl active community-set	Displays the community sets that are referenced by at least one policy that is being used at an attach point.
show rpl active extcommunity-set	Displays the extended community sets that are referenced by at least one policy that is being used at an attach point.
show rpl active route-policy	Displays the route policies that are referenced by at least one policy that is being used at an attach point.

R3.3 Beta Draft—Cisco Confidential Information

show rpl as-path-set

To display the contents of AS path sets, use the **show rpl as-path-set** command in EXEC mode.

show rpl as-path-set [*name* | *states* | *brief*]

Syntax Description	<i>name</i>	(Optional) Name of the AS path set.
	states	(Optional) Shows all unused, inactive, and active states.
	brief	(Optional) Limits the display to a list of the names of all AS path sets without their configurations.

Defaults No default behavior or value

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The summary keyword was replaced with brief . The * keyword was removed and the states keyword was added.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the optional **brief** keyword to limit the display to a list of the names of all AS path sets without their configurations.

Task ID	Task ID	Operations
	route-policy	read

Examples This example shows the following sample configuration:

```
RP/0/RP0/CPU0:router# show rpl route-policy policy_1

route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
```

R3.3 Beta Draft—Cisco Confidential Information

```

    set community (10:333) additive
  endif
end-policy

```

Given this sample configuration, the **show rpl as-path-set as_path_set_ex1** command displays the following information:

```

RP/0/RP0/CPU0:router# show rpl as-path-set as_path_set_ex1

as-path-set as_path_set_ex1
  ios-regex '^_65500_$',
  ios-regex '^_65501_$'
end-set

```

Related Commands	Command	Description
	show rpl community-set	Displays the configuration of a named community set.
	show rpl extcommunity-set	Displays the configuration of a named extended community set.
	show rpl route-policy	Displays the configuration of a named route policy.
	show rpl prefix-set	Displays the configuration of a named prefix set.

R3.3 Beta Draft—Cisco Confidential Information

show rpl as-path-set attachpoints

To display all of the policies used at an attach point that reference the named AS path set, use the **show rpl as-path-set attachpoints** command in EXEC mode.

show rpl as-path-set *name* **attachpoints**

Syntax Description	<i>name</i> Name of an AS path set.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **show rpl as-path-set attachpoints** command to display all policies used at an attach point that reference the named set either directly or indirectly.

The AS path set name is required.

Task ID	Task ID	Operations
	route-policy	read

Examples	This example shows the following sample configuration:

```
router bgp 2
 address-family ipv4 unicast
 !
 neighbor 10.0.101.2
  remote-as 100
  address-family ipv4 unicast
   route-policy policy_1 in
 !
 !
 neighbor 10.0.101.3
```

R3.3 Beta Draft—Cisco Confidential Information

```

remote-as 12
address-family ipv4 unicast
route-policy policy_2 in
!
!
!

RP/0/RP0/CPU0:router# show rpl route-policy policy_1

route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!
RP/0/RP0/CPU0:router# show rpl route-policy policy_2

route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy
!
```

Given this sample configuration, the **show rpl as-path-set as_path_set_ex1 attachpoints** command displays the following information:

```

RP/0/RP0/CPU0:router# show rpl as-path-set as_path_set_ex1 attachpoints

BGP Attachpoint:Neighbor

Neighbor/Group  type  afi/safi  in/out  referring policy  attached policy
-----
10.0.101.2      --    IPv4/uni  in      policy_1          policy_1
10.0.101.3      --    IPv4/uni  in      policy_2          policy_2
```

Table 133 describes the significant fields shown in the display.

Table 133 *show rpl as-path-set attachpoints Field Descriptions*

Field	Description
BGP Attachpoint	Location of the attach point.
Neighbor/Group	IP address of the attach point on the neighbor.
type	Displays the address family mode.
afi/safi	Address family identifier or subsequent address family identifier.
in/out	Import or export policy.
referring policy	Policy that refers to the AS path set.
attached policy	Policy used at the attach point.

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	show rpl community-set attachpoints	Displays all of the policies used at an attach point that reference the named community set.
	show rpl extcommunity-set attachpoints	Displays all of the policies used at an attach point that reference the named extended community set.
	show rpl route-policy attachpoints	Displays all of the policies used at an attach point that reference the named policy.
	show rpl prefix-set attachpoints	Displays all of the policies used at an attach point that reference the named prefix set.

R3.3 Beta Draft—Cisco Confidential Information

show rpl as-path-set references

To list all of the policies that reference the named AS path set, use the **show rpl as-path-set references** command in EXEC mode.

show rpl as-path-set *name* **references** [**brief**]

Syntax Description

<i>name</i>	Name of the prefix set.
brief	(Optional) Limits the output to just the brief table and not the detailed information for the named AS path set.

Defaults

No default behavior or value

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The summary keyword was replaced with brief .
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show rpl as-path-set references** command to display all policies that reference the named AS path set either directly or indirectly.

Use the optional **brief** keyword to limit the output to just a summary table and not the detailed information for the AS path set.

Task ID

Task ID	Operations
route-policy	read

Examples

This example shows the following sample configuration:

```
router bgp 2
 address-family ipv4 unicast
 !
 neighbor 10.0.101.2
 remote-as 100
 address-family ipv4 unicast
```

R3.3 Beta Draft—Cisco Confidential Information

```

    route-policy policy_1 in
    !
    !
RP/0/RP0/CPU0:router# show rpl route-policy policy_1

route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy

```

Given this sample configuration, the **show rpl as-path-set as_path_set_ex1 references** command displays the following information:

```
RP/0/RP0/CPU0:router# show rpl as-path-set as_path_set_ex1 references
```

```

Usage Direct -- Reference occurs in this policy
Usage Indirect -- Reference occurs via an apply statement

Status UNUSED -- Policy is not in use at an attachpoint (unattached)
Status ACTIVE -- Policy is actively used at an attachpoint
Status INACTIVE -- Policy is applied by an unattached policy

```

Usage/Status	count	
-----	-----	
Direct	1	
Indirect	0	
ACTIVE	1	
INACTIVE	0	
UNUSED	0	
route-policy	usage	policy status
-----	-----	-----
policy_1	Direct	ACTIVE

Table 134 describes the significant fields shown in the display.

Table 134 *show rpl as-path-set references Field Descriptions*

Field	Description
Usage/Status	Displays the usage and status of all policies that reference the AS path set. Values for usage are Direct or Indirect. Values for policy status are ACTIVE, INACTIVE, or UNUSED.
count	Number of policies that match each usage and status option.
route-policy	Name of the route policies that reference the AS path set.
usage	Type of usage for the policy.
policy status	Status of the policy.

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	show rpl community-set references	Lists all policies that reference the named community set.
	show rpl extcommunity-set references	Lists all policies that reference the named extended community set.
	show rpl route-policy references	Lists all policies that reference the named policy.
	show rpl prefix-set references	Lists all policies that reference the named prefix set.

R3.3 Beta Draft—Cisco Confidential Information

show rpl community-set

To display the configuration of community sets, use the **show rpl community-set** command in EXEC mode.

show rpl community-set [*name* | **states** | **brief**]

Syntax Description	<i>name</i>	(Optional) Name of the community set.
	states	(Optional) Shows all unused, inactive, and active states.
	brief	(Optional) Limits the display to a list of the names of all community sets without their configurations.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The summary keyword was replaced with brief . The * keyword was removed and the states keyword was added.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>. Use the optional brief keyword to limit the display to a list of the names of community sets without their configurations.

Task ID	Task ID	Operations
	route-policy	read

Examples	This example shows the following sample configuration: <pre>route-policy policy_4 if (destination in prefix_set_ex2) then if (community matches-any comm_set_ex2) then set community (10:666) additive endif if (extcommunity matches-any ext_comm_set_ex2) then</pre>

R3.3 Beta Draft – Cisco Confidential Information

```

        set community (10:999) additive
    endif
endif
end-policy

```

Given this sample configuration, the **show rpl community-set comm_set_ex2** command displays the following information:

```

RP/0/RP0/CPU0:router# show rpl community-set comm_set_ex2

community-set comm_set_ex2
  65501:1,
  65501:2,
  65501:3
end-set

```

Related Commands

Command	Description
show rpl as-path-set	Displays the configuration of a named AS path set.
show rpl extcommunity-set	Displays the configuration of a named extended community set.
show rpl route-policy	Displays the configuration of a named route policy.
show rpl prefix-set	Displays the configuration of a named prefix set.

R3.3 Beta Draft—Cisco Confidential Information

show rpl community-set attachpoints

To display all of the policies used at an attach point that reference the named community set, use the **show rpl community-set attachpoints** command in EXEC mode.

show rpl community-set *name* **attachpoints**

Syntax Description	<i>name</i> Name of a community set.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **show rpl community-set attachpoints** command to display all of the policies used at an attach point that reference the named community set either directly or indirectly.

The community set name is required.

Task ID	Task ID	Operations
	route-policy	read

Examples	This example shows the following sample configuration:

```
router bgp 2
 address-family ipv4 unicast
 !
 neighbor 10.0.101.3
  remote-as 12
  address-family ipv4 unicast
   route-policy policy_2 in
 !
 !
 route-policy policy_2
```

R3.3 Beta Draft – Cisco Confidential Information

```

if (destination in prefix_set_ex1) then
  if (community matches-any comm_set_ex1) then
    set community (10:666) additive
  endif
  if (extcommunity matches-any ext_comm_set_ex1) then
    set community (10:999) additive
  endif
endif
end-policy

```

Given this sample configuration, the **show rpl community-set comm_set_ex1 attachpoints** command displays the following information:

```
RP/0/RP0/CPU0:router# show rpl community-set comm_set_ex1 attachpoints
```

```
BGP Attachpoint:Neighbor
```

```

Neighbor/Group  type  afi/safi  in/out  referring policy  attached policy
-----
10.0.101.3      --   IPv4/uni  in      policy_2          policy_2

```

Table 135 describes the significant fields shown in the display.

Table 135 *show rpl community-set attachpoints Field Descriptions*

Field	Description
BGP Attachpoint	Location of the attach point.
Neighbor/Group	IP address of the attach point on the neighbor.
type	Displays the address family mode.
afi/safi	Address family identifier or subsequent address family identifier.
in/out	Import or export policy.
referring policy	Policy that refers to the AS path set.
attached policy	Policy used at the attach point.

Related Commands

Command	Description
show rpl as-path-set attachpoints	Displays all of the policies used at an attach point that reference the named AS path set.
show rpl extcommunity-set attachpoints	Displays all of the policies used at an attach point that reference the named extended community set.
show rpl route-policy attachpoints	Displays all of the policies used at an attach point that reference the named policy.
show rpl prefix-set attachpoints	Displays all of the policies used at an attach point that reference the named prefix set.

R3.3 Beta Draft—Cisco Confidential Information

show rpl community-set references

To list all of the policies that reference the named community set, use the **show rpl community-set references** command in EXEC mode.

show rpl community-set *name* **references** [**brief**]

Syntax Description

<i>name</i>	Name of a community set.
brief	(Optional) Limits the output to just the summary table and not the detailed information for the community set.

Defaults

No default behavior or value

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The summary keyword was replaced with brief .
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show rpl community-set references** command to display all of the policies that reference the named community set.

Use the optional **brief** keyword to limit the output to just a summary table and not the detailed information for the community set.

Task ID

Task ID	Operations
route-policy	read

Examples

This example shows the following sample configuration:

```
router bgp 2
 address-family ipv4 unicast
 !
 neighbor 10.0.101.3
 remote-as 12
 address-family ipv4 unicast
```


R3.3 Beta Draft—Cisco Confidential Information

```

route-policy policy_2 in
!
!
!
route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy

```

Given this sample configuration, the **show rpl community-set comm_set_ex1 references** command displays the following information:

```
RP/0/RP0/CPU0:router# show rpl community-set comm_set_ex1 references
```

Usage Direct -- Reference occurs in this policy

Usage Indirect -- Reference occurs via an apply statement

Status UNUSED -- Policy is not in use at an attachpoint (unattached)

Status ACTIVE -- Policy is actively used at an attachpoint

Status INACTIVE -- Policy is applied by an unattached policy

Usage/Status	count
Direct	1
Indirect	0
ACTIVE	1
INACTIVE	0
UNUSED	0

route-policy	usage	policy status
policy_2	Direct	ACTIVE

Table 136 describes the significant fields shown in the display.

Table 136 *show rpl community-set references Field Descriptions*

Field	Description
Usage/Status	Displays the usage and status of all policies that reference the community set. Values for usage are Direct or Indirect. Values for status are ACTIVE, INACTIVE, and UNUSED.
count	Number of policies that match each usage and status option.
route-policy	Name of the route policies that reference the community set.
usage	Type of usage for the policy.
policy status	Status of the policy.

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	show rpl as-path-set references	Lists all policies that reference the named AS path set.
	show rpl extcommunity-set references	Lists all policies that reference the named extended community set.
	show rpl route-policy references	Lists all policies that reference the named policy.
	show rpl prefix-set references	Lists all policies that reference the named prefix set.

R3.3 Beta Draft—Cisco Confidential Information

show rpl extcommunity-set

To display the configuration of extended community sets, use the **show rpl extcommunity-set** command in EXEC mode.

show rpl extcommunity-set [*name* | *states* | *brief*]

Syntax Description	name	(Optional) Name of the community set.
	states	(Optional) Shows all unused, inactive, and active states.
	brief	(Optional) Limits the display to a list of the names of all extended community sets without their configurations.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The summary keyword was replaced with brief . The * keyword was removed and the states keyword was added.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the optional brief keyword to limit the display to a list of the names of extended community sets without their configurations.

Task ID	Task ID	Operations
	route-policy	read

Examples	In the following example, the configuration of an extended community set extcommset_1 is displayed.
	<pre>RP/0/RP0/CPU0:router# show rpl extcommunity-set extcommset_1 extcommunity-set extcommset_1 SOO:10:2, SOO:10.0.0.1:24,</pre>

 `show rpl extcommunity-set`

R3.3 Beta Draft – Cisco Confidential Information

```
RT:10.0.0.5:10
end-set
```

Related Commands

Command	Description
show rpl as-path-set	Displays the configuration of a named AS path set.
show rpl community-set	Displays the configuration of a named community set.
show rpl route-policy	Displays the configuration of a named route policy.
show rpl prefix-set	Displays the configuration of a named prefix set.

R3.3 Beta Draft—Cisco Confidential Information

show rpl extcommunity-set attachpoints

To display all of the policies used at an attach point that reference the named extended community set, use the **show rpl extcommunity-set attachpoints** command in EXEC mode.

show rpl extcommunity-set *name* **attachpoints**

Syntax Description

<i>name</i>	Name of an extended community set.

Defaults

No default behavior or value

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show rpl extcommunity-set attachpoints** command to display all of the policies used at an attach point that reference the named extended community set either directly or indirectly.

The extended community set name is required.

Task ID

Task ID	Operations
route-policy	read

Examples

This example shows the following sample configuration:

```
router bgp 2
  address-family ipv4 unicast
  !
  neighbor 10.0.101.2
    remote-as 100
    address-family ipv4 unicast
    route-policy policy_1 in
  !
  neighbor 10.0.101.3
    remote-as 12
```

R3.3 Beta Draft—Cisco Confidential Information

```

address-family ipv4 unicast
  route-policy policy_2 in
!
!
!

RP/0/RP0/CPU0:router# show rpl route-policy policy_1

route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!
RP/0/RP0/CPU0:router# show rpl route-policy policy_2

route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy
!
```

Given this sample configuration, the **show rpl extcommunity-set ext_comm_set_ex1 attachpoints** command displays the following information:

```

RP/0/RP0/CPU0:router# show rpl extcommunity-set ext_comm_set_ex1 attachpoints

BGP Attachpoint:Neighbor

Neighbor/Group  type  afi/safi  in/out  referring policy  attached policy
-----
10.0.101.2      --   IPv4/uni  in      policy_1         policy_1
10.0.101.3      --   IPv4/uni  in      policy_2         policy_2
```

Table 137 describes the significant fields shown in the display.

Table 137 *show rpl extcommunity-set attachpoints Field Descriptions*

Field	Description
BGP Attachpoint	Location of the attach point.
Neighbor/Group	IP address of the attach point on the neighbor.
type	Displays the address family mode.
afi/safi	Address family identifier or subsequent address family identifier.
in/out	Import or export policy.
referring policy	Policy that refers to the AS path set.
attached policy	Policy used at the attach point.

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	show rpl as-path-set attachpoints	Displays all of the policies used at an attach point that reference the named AS path set.
	show rpl community-set attachpoints	Displays all of the policies used at an attach point that reference the named community set.
	show rpl route-policy attachpoints	Displays all of the policies used at an attach point that reference the named policy.
	show rpl prefix-set attachpoints	Displays all of the policies used at an attach point that reference the named prefix set.

R3.3 Beta Draft—Cisco Confidential Information

show rpl extcommunity-set references

To list all of the policies that reference the named community set, use the **show rpl extcommunity-set references** command in EXEC mode.

show rpl extcommunity-set *name* **references** [**brief**]

Syntax Description

name	Name of an extended community set.
brief	(Optional) Limits the output to just a summary table and not the detailed information for the extended community set.

Defaults

No default behavior or value

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The summary keyword was replaced with brief .
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show rpl extcommunity-set references** command to display all of the policies that reference the named extended community set either directly or indirectly.

Use the optional **brief** keyword to limit the output to just a summary table and not the detailed information for the extended community set.

Task ID

Task ID	Operations
route-policy	read

Examples

This example shows the following sample configuration:

```
router bgp 2
 address-family ipv4 unicast
 !
 neighbor 10.0.101.3
 remote-as 12
 address-family ipv4 unicast
```


R3.3 Beta Draft—Cisco Confidential Information

```

route-policy policy_2 in
!
!
!
route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy
!

```

Given this sample configuration, the **show rpl extcommunity-set ext_comm_set_ex1 references** command displays the following information.

```
RP/0/RP0/CPU0:router# show rpl extcommunity-set ext_comm_set_ex1 references
```

Usage Direct -- Reference occurs in this policy

Usage Indirect -- Reference occurs via an apply statement

Status UNUSED -- Policy is not in use at an attachpoint (unattached)

Status ACTIVE -- Policy is actively used at an attachpoint

Status INACTIVE -- Policy is applied by an unattached policy

Usage/Status	count
-----	-----
Direct	1
Indirect	0
ACTIVE	1
INACTIVE	0
UNUSED	0

route-policy	usage	policy status
-----	-----	-----
policy_2	Direct	ACTIVE

Table 138 describes the significant fields shown in the display.

Table 138 *show rpl extcommunity-set references Field Descriptions*

Field	Description
Usage/Status	Displays the usage and status of all policies that reference the extended community set. Values for usage are Direct or Indirect. Values for status are ACTIVE, INACTIVE, and UNUSED.
count	Number of policies that match each usage and status option.
route-policy	Name of the route policies that reference the extended community set.
usage	Type of usage for the policy.
policy status	Status of the policy.

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	show rpl as-path-set references	Lists all policies that reference the named AS path set.
	show rpl community-set references	Lists all policies that reference the named community set.
	show rpl route-policy references	Lists all policies that reference the named policy.
	show rpl prefix-set references	Lists all policies that reference the named prefix set.

R3.3 Beta Draft—Cisco Confidential Information

show rpl inactive as-path-set

To display the AS path sets that are referenced by a policy but not in any policy that is used at an attach point, use the **show rpl inactive as-path-set** command in EXEC mode.

show rpl inactive as-path-set

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or value

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show rpl inactive as-path-set** command to display all AS path sets that are not in use at an attach point either directly or indirectly, but are referenced by at least one policy in the system.

Task ID	Task ID	Operations
	route-policy	read

Examples This example shows the following sample configuration:

```
router bgp 2
 address-family ipv4 unicast
 !
 neighbor 10.0.101.2
  remote-as 100
  address-family ipv4 unicast
   route-policy policy_1 in
 !
 !
 neighbor 10.0.101.3
  remote-as 12
  address-family ipv4 unicast
   route-policy policy_2 in
```

R3.3 Beta Draft—Cisco Confidential Information

```

!
!
!
route-policy sample
  if (destination in sample) then
    drop
  endif
end-policy
!
route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy
!
route-policy policy_3
  if (destination in prefix_set_ex2) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex2) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_4
  if (destination in prefix_set_ex2) then
    if (community matches-any comm_set_ex2) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex2) then
      set community (10:999) additive
    endif
  endif
end-policy
!
route-policy policy_5
  apply martians
  apply policy_3
end-policy

```

Given this sample configuration, the **show rpl inactive as-path-set** command displays the following information:

```
RP/0/RP0/CPU0:router# show rpl inactive as-path-set
```

```

ACTIVE -- Referenced by at least one policy which is attached
INACTIVE -- Only referenced by policies which are not attached
UNUSED -- Not attached (directly or indirectly) and not referenced

```

R3.3 Beta Draft – Cisco Confidential Information

```
The following as-path-sets are INACTIVE
-----
as_path_set_ex2
```

Related Commands	Command	Description
	show rpl inactive community-set	Displays the community sets that are referenced by a policy but not in any policy that is used at an attach point.
	show rpl inactive extcommunity-set	Displays the extended community sets that are referenced by a policy but not in any policy that is used at an attach point.
	show rpl inactive prefix-set	Displays the route policies that are referenced by a policy but not in any policy that is used at an attach point.
	show rpl inactive prefix-set	Displays the prefix sets that are referenced by a policy but not in any policy that is used at an attach point.

R3.3 Beta Draft—Cisco Confidential Information

show rpl inactive community-set

To display the community sets that are referenced by a policy but not any policy that is used at an attach point, use the **show rpl inactive community-set** command in EXEC mode.

show rpl inactive community-set

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **show rpl inactive community-set** command to display all community sets that are not in use at an attach point either directly or indirectly, but are referenced by at least one policy in the system.

Task ID	Task ID	Operations
	route-policy	read

Examples	This example shows the following sample configuration:

```
router bgp 2
 address-family ipv4 unicast
 !
 neighbor 10.0.101.2
  remote-as 100
  address-family ipv4 unicast
   route-policy policy_1 in
 !
 !
 neighbor 10.0.101.3
  remote-as 12
  address-family ipv4 unicast
   route-policy policy_2 in
```

R3.3 Beta Draft—Cisco Confidential Information

```

!
!
!
route-policy sample2
  if (destination in sample2) then
    drop
  endif
end-policy
!
route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy
!
route-policy policy_3
  if (destination in prefix_set_ex2) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex2) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_4
  if (destination in prefix_set_ex2) then
    if (community matches-any comm_set_ex2) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex2) then
      set community (10:999) additive
    endif
  endif
end-policy
!
route-policy policy_5
  apply sample2
  apply policy_3
end-policy

```

Given this sample configuration, the **show rpl inactive community-set** command displays the following information:

```
RP/0/RP0/CPU0:router# show rpl inactive community-set
```

```

ACTIVE -- Referenced by at least one policy which is attached
INACTIVE -- Only referenced by policies which are not attached
UNUSED -- Not attached (directly or indirectly) and not referenced

```

■ `show rpl inactive community-set`

R3.3 Beta Draft – Cisco Confidential Information

The following community-sets are INACTIVE

comm_set_ex2

Related Commands	Command	Description
	show rpl inactive as-path-set	Displays the AS path sets that are referenced by a policy but not in any policy that is used at an attach point.
	show rpl inactive extcommunity-set	Displays the extended community sets that are referenced by a policy but not in any policy that is used at an attach point.
	show rpl inactive prefix-set	Displays the route policies that are referenced by a policy but not in any policy that is used at an attach point.
	show rpl inactive prefix-set	Displays the prefix sets that are referenced by a policy but not in any policy that is used at an attach point.

R3.3 Beta Draft—Cisco Confidential Information

show rpl inactive extcommunity-set

To display the extended community sets that are referenced by a policy but not in any policy that is used at an attach point, use the **show rpl inactive extcommunity-set** command in EXEC mode.

show rpl inactive extcommunity-path-set

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **show rpl inactive extcommunity-set** command to display all extended community sets that are not in use at an attach point either directly or indirectly, but are referenced by at least one policy in the system.

Task ID	Task ID	Operations
	route-policy	read

Examples	This example shows the following sample configuration:

```
router bgp 2
  address-family ipv4 unicast
  !
  neighbor 10.0.101.2
    remote-as 100
    address-family ipv4 unicast
    route-policy policy_1 in
  !
  !
  neighbor 10.0.101.3
    remote-as 12
```

R3.3 Beta Draft—Cisco Confidential Information

```

address-family ipv4 unicast
  route-policy policy_2 in
!
!
!
route-policy sample3
  if (destination in sample3) then
    drop
  endif
end-policy
!
route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy
!
route-policy policy_3
  if (destination in prefix_set_ex2) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex2) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_4
  if (destination in prefix_set_ex2) then
    if (community matches-any comm_set_ex2) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex2) then
      set community (10:999) additive
    endif
  endif
end-policy
!
route-policy policy_5
  apply sample3
  apply policy_3
end-policy

```

Given this sample configuration, the **show rpl inactive extcommunity-set** command displays the following information:

```
RP/0/RP0/CPU0:router# show rpl inactive extcommunity-set
```

```

ACTIVE -- Referenced by at least one policy which is attached
INACTIVE -- Only referenced by policies which are not attached
UNUSED -- Not attached (directly or indirectly) and not referenced

```

R3.3 Beta Draft – Cisco Confidential Information

```
The following extcommunity-sets are INACTIVE
-----
ext_comm_set_ex2
```

Related Commands	Command	Description
	show rpl inactive as-path-set	Displays the AS path sets that are referenced by a policy but not in any policy that is used at an attach point.
	show rpl inactive community-set	Displays the community sets that are referenced by a policy but not in any policy that is used at an attach point.
	show rpl inactive prefix-set	Displays the route policies that are referenced by a policy but not in any policy that is used at an attach point.
	show rpl inactive prefix-set	Displays the prefix sets that are referenced by a policy but not in any policy that is used at an attach point.

R3.3 Beta Draft—Cisco Confidential Information

show rpl inactive prefix-set

To display the prefix sets that are referenced by a policy but not in any policy that is used at an attach point, use the **show rpl inactive prefix-set** command in EXEC mode.

show rpl inactive prefix-set

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **show rpl inactive prefix-set** command to display all prefix sets that are not in use at an attach point either directly or indirectly, but are referenced by at least one policy in the system.

Task ID	Task ID	Operations
	route-policy	read

Examples	This example shows the following sample configuration:

```
router bgp 2
 address-family ipv4 unicast
 !
 neighbor 10.0.101.2
  remote-as 100
  address-family ipv4 unicast
   route-policy policy_1 in
 !
 !
 neighbor 10.0.101.3
  remote-as 12
  address-family ipv4 unicast
   route-policy policy_2 in
```

R3.3 Beta Draft—Cisco Confidential Information

```

!
!
!
route-policy sample4
  if (destination in sample4) then
    drop
  endif
end-policy
!
route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy
!
route-policy policy_3
  if (destination in prefix_set_ex2) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex2) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_4
  if (destination in prefix_set_ex2) then
    if (community matches-any comm_set_ex2) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex2) then
      set community (10:999) additive
    endif
  endif
end-policy
!
route-policy policy_5
  apply sample4
  apply policy_3
end-policy

```

Given this sample configuration, the **show rpl inactive prefix-set** command displays the following information:

```
RP/0/RP0/CPU0:router# show rpl inactive prefix-set
```

```

ACTIVE -- Referenced by at least one policy which is attached
INACTIVE -- Only referenced by policies which are not attached
UNUSED -- Not attached (directly or indirectly) and not referenced

```

■ **show rpl inactive prefix-set**

R3.3 Beta Draft – Cisco Confidential Information

The following prefix-sets are INACTIVE

sample4

prefix_set_ex2

Related Commands	Command	Description
	show rpl inactive as-path-set	Displays the AS path sets that are referenced by a policy but not in any policy that is used at an attach point.
	show rpl inactive community-set	Displays the community sets that are referenced by a policy but not in any policy that is used at an attach point.
	show rpl inactive extcommunity-set	Displays the extended community sets that are referenced by a policy but not in any policy that is used at an attach point.
	show rpl inactive prefix-set	Displays the route policies that are referenced by a policy but not in any policy that is used at an attach point.

R3.3 Beta Draft—Cisco Confidential Information

show rpl inactive route-policy

To display the route policies that are referenced by a policy but not in any policy that is used at an attach point, use the **show rpl inactive route-policy** command in EXEC mode.

show rpl inactive route-policy

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The policy keyword was changed to route-policy .
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **show rpl inactive route-policy** command to display all policies that are not in use at an attach point either directly or indirectly, but are referenced by at least one other policy in the system.

Task ID	Task ID	Operations
	route-policy	read

Examples	This example shows the following sample configuration:

```
router bgp 2
  address-family ipv4 unicast
  !
  neighbor 10.0.101.2
    remote-as 100
    address-family ipv4 unicast
    route-policy policy_1 in
  !
  !
  neighbor 10.0.101.3
    remote-as 12
```

R3.3 Beta Draft—Cisco Confidential Information

```

address-family ipv4 unicast
  route-policy policy_2 in
!
!
!
route-policy sample3
  if (destination in sample3) then
    drop
  endif
end-policy
!
route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy
!
route-policy policy_3
  if (destination in prefix_set_ex2) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex2) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_4
  if (destination in prefix_set_ex2) then
    if (community matches-any comm_set_ex2) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex2) then
      set community (10:999) additive
    endif
  endif
end-policy
!
route-policy policy_5
  apply sample3
  apply policy_3
end-policy

```

Given this sample configuration, the **show rpl inactive route-policy** command displays the following information:

```
RP/0/RP0/CPU0:router# show rpl inactive route-policy
```

```

ACTIVE -- Referenced by at least one policy which is attached
INACTIVE -- Only referenced by policies which are not attached
UNUSED -- Not attached (directly or indirectly) and not referenced

```


R3.3 Beta Draft – Cisco Confidential Information

```
The following policies are (INACTIVE)
-----
sample3
policy_3
```

Related Commands	Command	Description
	show rpl inactive as-path-set	Displays the AS path sets that are referenced by a policy but not in any policy that is used at an attach point.
	show rpl inactive community-set	Displays the community sets that are referenced by a policy but not in any policy that is used at an attach point.
	show rpl inactive extcommunity-set	Displays the extended community sets that are referenced by a policy but not in any policy that is used at an attach point.
	show rpl inactive prefix-set	Displays the prefix sets that are referenced by a policy but not in any policy that is used at an attach point.

R3.3 Beta Draft—Cisco Confidential Information

show rpl maximum

To display the maximum limits for lines of configuration and number of policies, use the **show rpl maximum** command in EXEC mode.

show rpl maximum [**lines** | **policies**]

Syntax Description

lines	(Optional) Displays the number of lines of configuration limit.
policies	(Optional) Displays the number of policies limit.

Defaults

No default behavior or value

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show rpl maximum** command to display the current total, current limit, and maximum limit for lines of configuration and policies.

Use the optional **lines** keyword to limit the display to the number of lines of configuration limits. Use the optional **policies** keyword to limit the display to the number of policies limits.

Task ID

Task ID	Operations
route-policy	read

Examples

In the following example, the **lines** keyword is used with the **show rpl maximum** command to display the number of lines of configuration limits:

```
RP/0/RP0/CPU0:router# show rpl maximum lines
```

	Current Total	Current Limit	Max Limit

Lines of configuration	58	65536	131072
Compiled policies size (kB)	10		

R3.3 Beta Draft – Cisco Confidential Information

Table 139 describes the significant fields shown in the display.

Table 139 *show rpl maximum Field Descriptions*

Field	Description
Lines of configuration	Displays the number of lines for the policy.
Compiled policies size (kB)	Displays the current compiled total for policies in kilobytes.

Related Commands

Command	Description
rpl maximum	Configures the maximum number of lines of configuration and number of policies.

R3.3 Beta Draft—Cisco Confidential Information

show rpl prefix-set

To display the configuration of prefix sets, use the **show rpl prefix-set** command in EXEC mode.

show rpl prefix-set [*name* | **states** | **brief**]

Syntax Description	<i>name</i>	(Optional) Name of the prefix set.
	states	(Optional) Shows all unused, inactive, and active states.
	brief	(Optional) Limits the display to a list of the names of all extended community sets without their configurations.

Defaults No default behavior or value

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The summary keyword was replaced with brief . The * keyword was removed and the states keyword was added.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Because sets cannot hierarchically reference other sets or policies, no **detail** keyword exists as with the **show rpl policy** command.

Task ID	Task ID	Operations
	route-policy	read

Examples In the following example, the configuration of prefix set pset1 is displayed:

```
RP/0/RP0/CPU0:router# show rpl prefix-set pset1
!
prefix-set pset1
  10.0.0.1/0,
  10.0.0.2/0 ge 25 le 32,
  10.0.0.5/8 ge 8 le 32,
  10.168.0.0/16 ge 16 le 32,
```

R3.3 Beta Draft – Cisco Confidential Information

```
172.16.0.9/20 ge 20 le 32,  
192.168.0.5/20 ge 20 le 32  
end-set
```

Related Commands

Command	Description
show rpl as-path-set	Displays the configuration of a named AS path set.
show rpl community-set	Displays the configuration of a named community set.
show rpl extcommunity-set	Displays the configuration of a named extended community set.
show rpl route-policy	Displays the configuration of a named route policy.

R3.3 Beta Draft—Cisco Confidential Information

show rpl prefix-set attachpoints

To display all of the policies used at an attach point that reference the named prefix set, use the **show rpl prefix-set attachpoints** command in EXEC mode.

show rpl prefix-set *name* **attachpoints**

Syntax Description	<i>name</i> Name of a prefix set.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **show rpl prefix-set attachpoints** command to display all of the policies used at an attach point that reference the named prefix set either directly or indirectly.

The prefix set name is required.

Task ID	Task ID	Operations
	route-policy	read

Examples	This example shows the following sample configuration:

```
router bgp 2
 address-family ipv4 unicast
 !
 neighbor 10.0.101.2
  remote-as 100
  address-family ipv4 unicast
   route-policy policy_1 in
 !
 !
 neighbor 10.0.101.3
  remote-as 12
```

R3.3 Beta Draft—Cisco Confidential Information

```

address-family ipv4 unicast
  route-policy policy_2 in
!
!
route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy

```

Given this sample configuration, the **show rpl prefix-set prefix_set_ex1 attachpoints** command displays the following information:

```
RP/0/RP0/CPU0:router# show rpl prefix-set prefix_set_ex1 attachpoints
```

```
BGP Attachpoint:Neighbor
```

Neighbor/Group	type	afi/safi	in/out	referring policy	attached policy
10.0.101.2	--	IPv4/uni	in	policy_1	policy_1
10.0.101.3	--	IPv4/uni	in	policy_2	policy_2

Table 140 describes the significant fields shown in the display.

Table 140 *show rpl prefix-set attachpoints Field Descriptions*

Field	Description
BGP Attachpoint	Location of the attach point.
Neighbor/Group	IP address of the attach point on the neighbor.
type	Address family mode.
afi/safi	Address family identifier or subsequent address family identifier.
in/out	Import or export policy.
referring policy	Policy that refers to the AS path set.
attached policy	Policy used at the attach point.

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	show rpl as-path-set attachpoints	Displays all of the policies used at an attach point that reference the named AS path set.
	show rpl community-set attachpoints	Displays all of the policies used at an attach point that reference the named community set.
	show rpl extcommunity-set attachpoints	Displays all of the policies used at an attach point that reference the named extended community set.
	show rpl route-policy attachpoints	Displays all of the policies used at an attach point that reference the named policy.

R3.3 Beta Draft—Cisco Confidential Information

show rpl prefix-set references

To list all of the policies that reference the named prefix set, use the **show rpl prefix-set references** command in EXEC mode.

show rpl prefix-set *name* **references** [**brief**]

Syntax Description	<i>name</i>	Name of the prefix set.
	brief	(Optional) Limits the output to just a summary table and not the detailed information for the named prefix set.

Defaults No default behavior or value

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The summary keyword was replaced with brief .
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show rpl prefix-set references** command to list all of the policies that reference the named prefix set.

Use the optional **brief** keyword to limit the output to just a summary table and not the detailed information for the named prefix set.

Task ID	Task ID	Operations
	route-policy	read

Examples Given the following sample configuration:

```
prefix-set ten-net
  10.0.0.0/16 le 32
end-set

prefix-set too-specific
  0.0.0.0/0 ge 25 le 32
```

R3.3 Beta Draft—Cisco Confidential Information

```

end-set
route-policy example-one
  if destination in ten-net then
    drop
  else
    set local-preference 200
    apply set-comms
  endif
end-policy
route-policy set-comms
  set community (10:1234) additive
end-policy

route-policy example-three
  if destination in too-specific then
    drop
  else
    apply example-one
    pass
  endif
end-policy

```

the following example displays information showing the usage and status of each policy that references the prefix set ten-net. The **brief** keyword limits the display to just a summary table and not the detailed information for the prefix set.

```
RP/0/RP0/CPU0:router# show rpl prefix-set ten-net references brief
```

Usage Direct -- Reference occurs in this policy

Usage Indirect -- Reference occurs via an apply statement

Status UNUSED -- Policy is not in use at an attachpoint (unattached)

Status ACTIVE -- Policy is actively used at an attachpoint

Status INACTIVE -- Policy is applied by an unattached policy

Usage/Status	count
Direct	1
Indirect	1
ACTIVE	0
INACTIVE	1
UNUSED	1

Table 141 describes the significant fields shown in the display.

Table 141 *show rpl prefix-set name references Field Descriptions*

Field	Description
Usage/Status	Displays the usage and status of all policies that reference the prefix set.
count	Number of policies that match each usage and status option.

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	show rpl as-path-set references	Lists all of the policies that reference the named AS path set.
	show rpl community-set references	Lists all of the policies that reference the named community set.
	show rpl extcommunity-set references	Lists all of the policies that reference the named extended community set.
	show rpl route-policy references	Lists all of the policies that reference the named policy.

R3.3 Beta Draft—Cisco Confidential Information

show rpl route-policy

To display the configuration of route policies, use the **show rpl route-policy** command in EXEC mode.

show rpl route-policy [*name* [**detail**] | **states** | **brief**]

Syntax Description	<i>name</i>	(Optional) Name of a route policy.
	detail	(Optional) Displays the configuration of all policies and sets that a policy uses.
	states	(Optional) Shows all unused, inactive, and active states.
	brief	(Optional) Limits the display to a list of the names of all extended community sets without their configurations.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The summary keyword was replaced with brief . The policy keyword was changed to route-policy . The * keyword was removed and the states keyword was added.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the optional brief keyword to limit the display to a list of the names of policies without their configurations.

Task ID	Task ID	Operations
	route-policy	read

R3.3 Beta Draft—Cisco Confidential Information

Examples

In the following example, the configuration of a route policy named policy_1 is displayed.

```
RP/0/RP0/CPU0:router# show rpl route-policy policy_1

route-policy policy_1
  if destination in prefix_set_1 and not destination in martians then
    if as-path in aspath_set_1 then
      set local-preference 300
      set origin igp
    elseif as-path in as_allowed then
      set local-preference 400
      set origin igp
    else
      set origin igp
    endif
  else
    drop
  endif
  set med 120
  set community (8660:612) additive
  apply set_lpref_from_comm
end-policy
```

If the optional **detail** keyword is used, all routing policy language (RPL) policies and sets that route policy policy_1 uses are displayed, as shown in the following example.

```
RP/0/RP0/CPU0:router# show rpl route-policy policy_1 detail

!
prefix-set martians
  0.0.0.0/0,
  0.0.0.0/0 ge 25 le 32,
  10.0.0.0/8 ge 8 le 32,
  192.168.0.0/16 ge 16 le 32,
  224.0.0.0/20 ge 20 le 32,
  240.0.0.0/20 ge 20 le 32
end-set
!
prefix-set prefix_set_1
  10.0.0.1/24 ge 24 le 32,
  10.0.0.5/24 ge 24 le 32,
  172.16.0.1/24 ge 24 le 32,
  172.16.5.5/24 ge 24 le 32,
  172.16.20.10/24 ge 24 le 32,
  172.30.0.1/24 ge 24 le 32,
  10.0.20.10/24 ge 24 le 32,
  172.18.0.5/24 ge 24 le 32,
  192.168.0.1/24 ge 24 le 32,
  192.168.20.10/24 ge 24 le 32,
  192.168.200.10/24 ge 24 le 32,
  192.168.255.254/24 ge 24 le 32
end-set
!
as-path-set as_allowed
  ios-regex '.*_1239_.*',
  ios-regex '.*_3561_.*',
  ios-regex '.*_701_.*',
  ios-regex '.*_666_.*',
  ios-regex '.*_1755_.*',
  ios-regex '.*_1756_.*'
end-set
!
as-path-set aspath_set_1
  ios-regex '._9148_',
```

R3.3 Beta Draft—Cisco Confidential Information

```

ios-regex '_5870_',
ios-regex '_2408_',
ios-regex '_2531_',
ios-regex '_197_',
ios-regex '_2992_'
end-set
!
route-policy set_lpref_from_comm
  if community matches-any (2:50) then
    set local-preference 50
  elseif community matches-any (2:60) then
    set local-preference 60
  elseif community matches-any (2:70) then
    set local-preference 70
  elseif community matches-any (2:80) then
    set local-preference 80
  elseif community matches-any (2:90) then
    set local-preference 90
  endif
end-policy
!
route-policy policy_1
  if destination in prefix_set_1 and not destination in martians then
    if as-path in aspath_set_1 then
      set local-preference 300
      set origin igp
    elseif as-path in as_allowed then
      set local-preference 400
      set origin igp
    else
      set origin igp
    endif
  else
    drop
  endif
  set med 120
  set community (8660:612) additive
  apply set_lpref_from_comm
end-policy

```

Related Commands	Command	Description
	show rpl as-path-set	Displays the configuration of a named AS path set.
	show rpl community-set	Displays the configuration of a named community set.
	show rpl extcommunity-set	Displays the configuration of a named extended community set.
	show rpl prefix-set	Displays the configuration of a named prefix set.

R3.3 Beta Draft—Cisco Confidential Information

show rpl route-policy attachpoints

To display all of the policies used at an attach point that reference the named policy, use the **show rpl route-policy attachpoints** command in EXEC mode.

show rpl route-policy *name* **attachpoints**

Syntax Description	<i>name</i> Name of a policy.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The policy keyword was changed to route-policy .
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
	Use the show rpl route-policy attachpoints command to display all of the policies used at an attach point that reference the named policy either directly or indirectly.
	The policy name is required.

Task ID	Task ID	Operations
	route-policy	read

Examples	Given the following sample Border Gateway Protocol (BGP) configuration:

```
router bgp 2
 address-family ipv4 unicast
 !
 neighbor 10.0.101.2
  remote-as 100
  address-family ipv4 unicast
   route-policy policy_1 in
 !
 !
```

R3.3 Beta Draft—Cisco Confidential Information

```

neighbor 10.0.101.3
remote-as 12
address-family ipv4 unicast
route-policy policy_2 in
!
!
!

RP/0/RP0/CPU0:router# show rpl route-policy policy_1

route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!
RP/0/RP0/CPU0:router# show rpl route-policy policy_2

route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy
!
```

The following command displays the following information:

```
RP/0/RP0/CPU0:router# show rpl route-policy policy_2 attachpoints
```

BGP Attachpoint: Neighbor

```

Neighbor/Group  type  afi/safi  in/out  referring policy  attached policy
-----
10.0.101.2      --   IPv4/uni  in      policy_1         policy_1
10.0.101.3      --   IPv4/uni  in      policy_2         policy_2
```

Table 142 describes the significant fields shown in the display.

Table 142 *show rpl route-policy attachpoints Field Descriptions*

Field	Description
BGP Attachpoint	Location of the attach point.
Neighbor/Group	IP address of the attach point on the neighbor.
type	Displays the address family mode.
afi/safi	Address family identifier or subsequent address family identifier.
in/out	Import or export policy.
referring policy	Policy that refers to the AS path set.
attached policy	Policy used at the attach point.

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	show rpl as-path-set attachpoints	Displays all of the policies used at an attach point that reference the named AS path set.
	show rpl community-set attachpoints	Displays all of the policies used at an attach point that reference the named community set.
	show rpl extcommunity-set attachpoints	Displays all of the policies used at an attach point that reference the named extended community set.
	show rpl prefix-set attachpoints	Displays all of the policies used at an attach point that reference the named prefix set.

R3.3 Beta Draft—Cisco Confidential Information

show rpl route-policy references

To list all of the policies that reference the named policy, use the **show rpl route-policy references** command in EXEC mode.

show rpl route-policy *name* **references** [**brief**]

Syntax Description

<i>name</i>	Name of a prefix set.
brief	(Optional) Limits the output to just a summary table and not the detailed information for the named policy.

Defaults

No default behavior or value

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The summary keyword was replaced with brief . The policy keyword was replaced with route-policy .
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show rpl route-policy references** command to list all of the policies that reference the named policy.

Use the optional **brief** keyword to limit the output to just a summary table and not the detailed information for the policy.

Task ID

Task ID	Operations
route-policy	read

Examples

Given the following sample configuration:

```
prefix-set ten-net
  10.0.0.0/16 le 32
end-set
prefix-set too-specific
```

R3.3 Beta Draft—Cisco Confidential Information

```

0.0.0.0/0 ge 25 le 32
end-set
route-policy example-one
  if destination in ten-net then
    drop
  else
    set local-preference 200
    apply set-comms
  endif
end-policy

route-policy set-comms
  set community (10:1234) additive
end-policy

route-policy example-three
  if destination in too-specific then
    drop
  else
    apply example-one
    pass
  endif
end-policy

```

The following command displays information about the policy set-comms and how it is referenced.

```
RP/0/RP0/CPU0:router# show rpl route-policy set-comms references
```

Usage Direct -- Reference occurs in this policy

Usage Indirect -- Reference occurs via an apply statement

Status UNUSED -- Policy is not in use at an attachpoint (unattached)

Status ACTIVE -- Policy is actively used at an attachpoint

Status INACTIVE -- Policy is applied by an unattached policy

Usage/Status	count
Direct	1
Indirect	1
ACTIVE	0
INACTIVE	1
UNUSED	1
route-policy	usage policy status
example-one	Direct INACTIVE
example-three	IndirectUNUSED

The direct usage indicates that the route policy example-one directly applies the policy set-comms, that is, example-one has a line in the form apply set-comms. The usage Indirect indicates that the route policy example-three does not directly apply the route policy set-comms. However, the route policy example-three does apply the policy example-one, which in turn applies the policy set-comms, so there is an indirect reference from example-three to the route policy set-comms.

The status column indicates one of three states. A policy is active if it is in use at an attach point. In the example provided, neither example-one nor example-three is in use at an attach point, which leaves two possible states: UNUSED or INACTIVE. The route policy example-one is inactive because it has some other policy (example-three) that references it, but neither example-one nor any of the policies that reference it (example-one) are in use at an attach point. The route policy example-three has a status of unused because it is not used at an attach point and no other route policies in the system refer to it.

R3.3 Beta Draft – Cisco Confidential Information

Table 143 describes the significant fields shown in the display.

Table 143 *show rpl route-policy references Field Descriptions*

Field	Description
Usage/Status	Displays the usage and status of all policies that reference the specified policy. Values for usage are Direct or Indirect. Values for status are ACTIVE, INACTIVE, and UNUSED.
count	Number of policies that match each usage and status option.
route-policy	One name for multiple policies that reference the specified policy.
usage	Type of usage for the policy.
policy status	Status of the policy.

Related Commands

Command	Description
show rpl as-path-set references	Lists all policies that reference the named AS path set.
show rpl community-set references	Lists all policies that reference the named community set.
show rpl extcommunity-set references	Lists all policies that reference the named extended community set.
show rpl prefix-set references	Lists all policies that reference the named prefix set.

R3.3 Beta Draft—Cisco Confidential Information

show rpl route-policy uses

To display information about a specified named policy, use the **show rpl route-policy uses** command in EXEC mode.

show rpl route-policy *name* **uses** {**policies** | **sets** | **all**} [**direct**]

Syntax Description	
<i>name</i>	Name of a policy.
policies	Generates a list of all policies that the named policy uses.
sets	Lists all named sets that are used by the policy.
all	Generates a list of both sets and policies that the named policy references.
direct	(Optional) Lists only the policies or sets used directly in the named policy block. Set or policy references that occur as a result of an apply statement are not listed.

Defaults No default behavior or value

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The policy keyword was changed to route-policy .
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show rpl route-policy uses** command to display information about a specified named policy.

Task ID	Task ID	Operations
	route-policy	read

Examples Given the following sample configuration:

```
prefix-set ten-net
  10.0.0.0/16 le 32
end-set

prefix-set too-specific
  0.0.0.0/0 ge 25 le 32
```

R3.3 Beta Draft—Cisco Confidential Information

```

end-set
route-policy example-one
  if destination in ten-net then
    drop
  else
    set local-preference 200
    apply set-comms
  endif
end-policy
route-policy set-comms
  set community (10:1234) additive
end-policy
route-policy example-three
  if destination in too-specific then
    drop
  else
    apply example-one
    pass
  endif
end-policy

```

the following command lists the policies one and set-comms. It also lists the prefix sets too-specific and ten-net.

```
RP/0/RP0/CPU0:router# show rpl route-policy example-three uses all
```

```
Policies directly and indirectly applied by this policy:
```

```
-----
example-one set-comms
```

```
Sets referenced directly and indirectly
```

```
-----
(via applied policies) in this policy:
```

```
type prefix-set:
  ten-net too-specific
```

The sets example-one and set-comms are listed as policies that are used by the policy example-three. The policy example-one is listed because route policy example-three uses it in an **apply** statement. The policy set-comms is also listed because example-one applies it. Similarly, the prefix-set too-specific is used directly in the **if** statement in the policy example-three, and the prefix-set ten-net is used in the policy example-one. The optional **direct** keyword can be used to limit the output to just those sets and policies that are used within the example-three block itself, as shown in the following example:

```
RP/0/RP0/CPU0:router# show rpl route-policy example-three uses all direct
```

```
Policies directly applied by this policy:
```

```
-----
example-one
```

```
Sets used directly in this policy
```

```
-----
type prefix-set:
  too-specific
```

As can be seen in the output, the route policy set-comms and the prefix set ten-net are no longer included in the output when the **direct** keyword is used. The **direct** form of the command considers only those sets or policies used in the specified route policy and any additional policies or sets that may be used if you follow the hierarchy of **apply** statements.

R3.3 Beta Draft—Cisco Confidential Information

Table 144 describes the significant fields shown in the display.

Table 144 *show rpl route-policy uses Field Descriptions*

Field	Description
type	Displays the type used in the policy configuration. Values for type are prefix-set, community-set, extcommunity-set, and as-path-set.

R3.3 Beta Draft—Cisco Confidential Information

show rpl unused as-path-set

To display the AS path sets that are defined but not used by a policy at an attach point or referenced in a policy using an **apply** statement, use the **show rpl unused as-path-set** command in EXEC mode.

show rpl unused as-path-set

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **show rpl unused as-path-set** command to display all AS path sets that are not used in a policy at an attach point either directly or indirectly, and are not referenced by any policies in the system.

Task ID	Task ID	Operations
	route-policy	read

Examples	This example shows the following sample configuration:

```
router bgp 2
 address-family ipv4 unicast
 !
 neighbor 10.0.101.2
  remote-as 100
  address-family ipv4 unicast
   route-policy policy_1 in
 !
 !
 neighbor 10.0.101.3
  remote-as 12
  address-family ipv4 unicast
   route-policy policy_2 in
```


R3.3 Beta Draft—Cisco Confidential Information

```

!
!
!
as-path-set as_path_set_ex1
  ios-regex '^_65500_$',
  ios-regex '^_65501_$'
end-set
!
as-path-set as_path_set_ex2
  ios-regex '^_65502_$',
  ios-regex '^_65503_$'
end-set
!
as-path-set as_path_set_ex3
  ios-regex '^_65504_$',
  ios-regex '^_65505_$'
end-set
!
route-policy sample
  if (destination in sample) then
    drop
  endif
end-policy
!
route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy
!
route-policy policy_3
  if (destination in prefix_set_ex2) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex2) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_4
  if (destination in prefix_set_ex2) then
    if (community matches-any comm_set_ex2) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex2) then
      set community (10:999) additive
    endif
  endif
end-policy
!

```

R3.3 Beta Draft – Cisco Confidential Information

```
route-policy policy_5
  apply sample
  apply policy_3
end-policy
```

Given this sample configuration, the **show rpl unused as-path-set** command displays the following information.

```
RP/0/RP0/CPU0:router# show rpl unused as-path-set

ACTIVE -- Referenced by at least one policy which is attached
INACTIVE -- Only referenced by policies which are not attached
UNUSED -- Not attached (directly or indirectly) and not referenced

The following as-path-sets are UNUSED
-----
as_path_set_ex3
```

Related Commands	show rpl unused community-set	Displays the community sets that are not referenced at all.
	show rpl unused extcommunity-set	Displays the extended community sets that are not referenced at all.
	show rpl unused prefix-set	Displays the prefix sets that are not referenced at all.

R3.3 Beta Draft—Cisco Confidential Information

show rpl unused community-set

To display the community sets that are defined but not used by a policy at an attach point or referenced in a policy using an **apply** statement, use the **show rpl unused community-set** command in EXEC mode.

show rpl unused community-set

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or value

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show rpl unused community-set** command to display all of the community sets that are not used in a policy at an attach point either directly or indirectly, and are not referenced by any policies in the system.

Task ID	Task ID	Operations
	route-policy	read

Examples This example shows the following sample configuration:

```
router bgp 2
 address-family ipv4 unicast
 !
 neighbor 10.0.101.2
  remote-as 100
  address-family ipv4 unicast
   route-policy policy_1 in
 !
 !
 neighbor 10.0.101.3
```

R3.3 Beta Draft—Cisco Confidential Information

```

remote-as 12
address-family ipv4 unicast
route-policy policy_2 in
!
!
!

community-set comm_set_ex1
65500:1,
65500:2,
65500:3
end-set
!
community-set comm_set_ex2
65501:1,
65501:2,
65501:3
end-set
!
community-set comm_set_ex3
65502:1,
65502:2,
65502:3
end-set
!
route-policy sample
if (destination in sample) then
drop
endif
end-policy
!
route-policy policy_1
if (destination in prefix_set_ex1) then
set local-preference 100
endif
if (as-path in as_path_set_ex1) then
set community (10:333) additive
endif
end-policy
!
route-policy policy_2
if (destination in prefix_set_ex1) then
if (community matches-any comm_set_ex1) then
set community (10:666) additive
endif
if (extcommunity matches-any ext_comm_set_ex1) then
set community (10:999) additive
endif
endif
end-policy
!
route-policy policy_3
if (destination in prefix_set_ex2) then
set local-preference 100
endif
if (as-path in as_path_set_ex2) then
set community (10:333) additive
endif
end-policy
!
route-policy policy_4
if (destination in prefix_set_ex2) then
if (community matches-any comm_set_ex2) then
set community (10:666) additive

```

R3.3 Beta Draft – Cisco Confidential Information

```

endif
if (extcommunity matches-any ext_comm_set_ex2) then
    set community (10:999) additive
endif
endif
end-policy
!
route-policy policy_5
    apply sample
    apply policy_3
end-policy

```

Given this sample configuration, the **show rpl unused community-set** command displays the following information.

```
RP/0/RP0/CPU0:router# show rpl unused community-set
```

```

ACTIVE -- Referenced by at least one policy which is attached
INACTIVE -- Only referenced by policies which are not attached
UNUSED -- Not attached (directly or indirectly) and not referenced

```

The following community-sets are UNUSED

```

-----
comm_set_ex3

```

Related Commands

Command	Description
show rpl unused as-path-set	Displays the AS path sets that are not referenced at all.
show rpl unused extcommunity-set	Displays the extended community sets that are not referenced at all.
show rpl unused prefix-set	Displays the prefix sets that are not referenced at all.

R3.3 Beta Draft—Cisco Confidential Information

show rpl unused extcommunity-set

To display the extended community sets that are defined but not used by a policy at an attach point or referenced in a policy using an **apply** statement, use the **show rpl unused extcommunity-set** command in EXEC mode.

show rpl unused extcommunity-set

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

Use the **show rpl unused extcommunity-set** command to display all extended community sets that are not used in a policy at an attach point either directly or indirectly, and are not referenced by any policies in the system.

Task ID	Task ID	Operations
	route-policy	read

Examples	This example shows the following sample configuration:

```
router bgp 2
 address-family ipv4 unicast
 !
 neighbor 10.0.101.2
  remote-as 100
  address-family ipv4 unicast
   route-policy policy_1 in
 !
 !
 neighbor 10.0.101.3
```

R3.3 Beta Draft—Cisco Confidential Information

```
remote-as 12
address-family ipv4 unicast
  route-policy policy_2 in
!
!
!
extcommunity-set ext_comm_set_ex1
  SOO:65500:1,
  RT:1.2.3.4:34
end-set
!
extcommunity-set ext_comm_set_ex2
  SOO:65501:1,
  RT:2.3.4.5:36
end-set
!
extcommunity-set ext_comm_set_ex3
  SOO:65502:1,
  RT:6.7.8.9:36
end-set
!
route-policy sample
  if (destination in sample) then
    drop
  endif
end-policy
!
route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy
!
route-policy policy_3
  if (destination in prefix_set_ex2) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex2) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_4
  if (destination in prefix_set_ex2) then
    if (community matches-any comm_set_ex2) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex2) then
      set community (10:999) additive
    endif
  endif
```

R3.3 Beta Draft – Cisco Confidential Information

```
endif
end-policy
!
route-policy policy_5
  apply sample
  apply policy_3
end-policy
```

Given this sample configuration, the **show rpl unused extcommunity-set** command displays the following information.

```
RP/0/RP0/CPU0:router# show rpl unused extcommunity-set
```

```
ACTIVE -- Referenced by at least one policy which is attached
INACTIVE -- Only referenced by policies which are not attached
UNUSED -- Not attached (directly or indirectly) and not referenced
```

The following extcommunity-sets are UNUSED

```
-----
ext_comm_set_ex3
```

Related Commands

Command	Description
show rpl unused as-path-set	Displays the AS path sets that are not referenced at all.
show rpl unused community-set	Displays community sets that are not referenced at all.
show rpl unused prefix-set	Displays prefix sets that are not referenced at all.

R3.3 Beta Draft—Cisco Confidential Information

show rpl unused prefix-set

To display the prefix sets that are defined but not used by a policy at an attach point or referenced in a policy using an **apply** statement, use the **show rpl unused prefix-set** command in EXEC mode.

show rpl unused prefix-set

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **show rpl unused prefix-set** command to display all prefix sets that are not used in a policy at an attach point either directly or indirectly, and are not referenced by any policies in the system.

Task ID	Task ID	Operations
	route-policy	read

Examples	This example shows the following sample configuration:

```
router bgp 2
  address-family ipv4 unicast
  !
  neighbor 10.0.101.2
    remote-as 100
    address-family ipv4 unicast
    route-policy policy_1 in
  !
  !
  neighbor 10.0.101.3
    remote-as 12
    address-family ipv4 unicast
    route-policy policy_2 in
```

R3.3 Beta Draft—Cisco Confidential Information

```

!
!
!

prefix-set sample
  0.0.0.0/0,
  0.0.0.0/0 ge 25 le 32,
  10.0.0.0/8 ge 8 le 32,
  192.168.0.0/16 ge 16 le 32,
  224.0.0.0/20 ge 20 le 32,
  240.0.0.0/20 ge 20 le 32
end-set
!
prefix-set prefix_set_ex1
  10.0.0.0/16 ge 16 le 32,
  0.0.0.0/0 ge 25 le 32,
  0.0.0.0/0
end-set
!
prefix-set prefix_set_ex2
  220.220.220.0/24 ge 24 le 32,
  220.220.120.0/24 ge 24 le 32,
  220.220.130.0/24 ge 24 le 32
end-set
!
prefix-set prefix_set_ex3
  221.221.220.0/24 ge 24 le 32,
  221.221.120.0/24 ge 24 le 32,
  221.221.130.0/24 ge 24 le 32
end-set
!
route-policy sample
  if (destination in sample) then
    drop
  endif
end-policy
!
route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
end-policy
!
route-policy policy_3
  if (destination in prefix_set_ex2) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex2) then
    set community (10:333) additive
  endif

```

R3.3 Beta Draft – Cisco Confidential Information

```

end-policy
!
route-policy policy_4
  if (destination in prefix_set_ex2) then
    if (community matches-any comm_set_ex2) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex2) then
      set community (10:999) additive
    endif
  endif
end-policy
!
route-policy policy_5
  apply sample
  apply policy_3
end-policy

```

Given this sample configuration, the **show rpl unused prefix-set** command displays the following information.

```
RP/0/RP0/CPU0:router# show rpl unused prefix-set
```

```

ACTIVE -- Referenced by at least one policy which is attached
INACTIVE -- Only referenced by policies which are not attached
UNUSED -- Not attached (directly or indirectly) and not referenced

```

```

The following prefix-sets are UNUSED
-----
prefix_set_ex3

```

Related Commands

Command	Description
show rpl unused as-path-set	Displays AS path sets that are not referenced at all.
show rpl unused community-set	Displays community sets that are not referenced at all.
show rpl unused extcommunity-set	Displays extended community sets that are not referenced at all.
show rpl unused prefix-set	Displays policies that are not referenced at all.

R3.3 Beta Draft—Cisco Confidential Information

show rpl unused route-policy

To display the route policies that are defined but not used at an attach point or referenced using an **apply** statement, use the **show rpl unused route-policy** command in EXEC mode.

show rpl unused route-policy

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or value

Command Modes	EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router. The policy keyword was changed to route-policy .
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Use the **show rpl unused route-policy** command to display route policies that are defined but not used at an attach point or referenced from another policy using an **apply** statement.

Task ID	Task ID	Operations
	route-policy	read

Examples	This example shows the following sample configuration:

```
RP/0/RP0/CPU0:router# show run | begin prefix-set
```

```
Building configuration...
prefix-set prefix_set_ex1
  10.0.0.0/16 ge 16 le 32,
  0.0.0.0/0 ge 25 le 32,
  0.0.0.0/0
end-set
!
prefix-set prefix_set_ex2
  220.220.220.0/24 ge 24 le 32,
```

R3.3 Beta Draft—Cisco Confidential Information

```
220.220.120.0/24 ge 24 le 32,
220.220.130.0/24 ge 24 le 32
end-set
!
as-path-set as_path_set_ex1
  ios-regex '^_65500_$',
  ios-regex '^_65501_$'
end-set
!
as-path-set as_path_set_ex2
  ios-regex '^_65502_$',
  ios-regex '^_65503_$'
end-set
!
as-path-set as_path_set_ex3
  ios-regex '^_65504_$',
  ios-regex '^_65505_$'
end-set
!
community-set comm_set_ex1
  65500:1,
  65500:2,
  65500:3
end-set
!
community-set comm_set_ex2
  65501:1,
  65501:2,
  65501:3
end-set
!
extcommunity-set ext_comm_set_ex1
  S00:65500:1,
  RT:1.2.3.4:34
end-set
!
extcommunity-set ext_comm_set_ex2
  S00:65501:1,
  RT:2.3.4.5:36
end-set
!
route-policy sample
  if (destination in sample) then
    drop
  endif
end-policy
!
route-policy policy_1
  if (destination in prefix_set_ex1) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex1) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_2
  if (destination in prefix_set_ex1) then
    if (community matches-any comm_set_ex1) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex1) then
      set community (10:999) additive
    endif
  endif
```

R3.3 Beta Draft—Cisco Confidential Information

```

endif
end-policy
!
route-policy policy_3
  if (destination in prefix_set_ex2) then
    set local-preference 100
  endif
  if (as-path in as_path_set_ex2) then
    set community (10:333) additive
  endif
end-policy
!
route-policy policy_4
  if (destination in prefix_set_ex2) then
    if (community matches-any comm_set_ex2) then
      set community (10:666) additive
    endif
    if (extcommunity matches-any ext_comm_set_ex2) then
      set community (10:999) additive
    endif
  endif
end-policy
!
route-policy policy_5
  apply sample
  apply policy_3
end-policy
!
route ipv4 0.0.0.0/0 10.91.37.129
route ipv4 10.91.36.0/23 10.91.37.129
route ipv4 10.91.38.0/24 10.91.37.129
end

```

In the following example, route policies that are defined but not used at an attach point or referenced from another policy using an **apply** statement are displayed using the **show rpl unused route-policy** command.

RP/0/RP0/CPU0:router# **show rpl unused route-policy**

ACTIVE -- Referenced by at least one policy which is attached
 INACTIVE -- Only referenced by policies which are not attached
 UNUSED -- Not attached (directly or indirectly) and not referenced

The following policies are (UNUSED)

```

-----
policy_1
policy_2
policy_4
policy_5

```

Related Commands

Command	Description
show rpl unused as-path-set	Displays AS path sets that are not referenced at all.
show rpl unused community-set	Displays community sets that are not referenced at all.
show rpl unused extcommunity-set	Displays extended community sets that are not referenced at all.
show rpl unused prefix-set	Displays prefix sets that are not referenced at all.

R3.3 Beta Draft—Cisco Confidential Information

source in

To test the source of a Border Gateway Protocol (BGP) route against the data in either a named or an inline prefix set, use the **source in** command in route-policy configuration mode.

source in {*prefix-set-name* | *inline-prefix-set*}

Syntax Description

<i>prefix-set-name</i>	Name of a prefix set.
<i>inline-prefix-set</i>	Inline prefix set.

Defaults

No default behavior or value

Command Modes

Route-policy configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **source in** command as a conditional expression within an **if** statement to test the source of the route against the data in either a named or an inline prefix set. A comparison that references a prefix set with zero elements in it returns false.

**Note**

For a list of all conditional expressions available within an **if** statement, see the **if** command.

The source of a BGP route is the IP peering address of the neighboring router from which the route was received.

The prefix set can contain both IPv4 and IPv6 prefix specifications.

Task ID

Task ID	Operations
route-policy	read, write

R3.3 Beta Draft – Cisco Confidential Information

Examples

In the following example, the source of a BGP route is tested against the data in the prefix set my-prefix-set:

```
RP/0/RP0/CPU0:router(config)# route-policy policy-A
RP/0/RP0/CPU0:router(config-rpl)# if source in my-prefix-set then
```

In this example, the source of a BGP route is tested against the data in an inline IPv4 prefix set:

```
RP/0/RP0/CPU0:router(config)# route-policy policy-B
RP/0/RP0/CPU0:router(config-rpl)# if source in (10.0.0.8, 10.0.0.20) then
```

In this example, the source of a route is tested against the data in an inline IPv6 prefix set:

```
RP/0/RP0/CPU0:router(config)# route-policy policy-C
RP/0/RP0/CPU0:router(config-rpl)# if source in (2001:0:0:1::/64, 2001:0:0:2::/64) then
```

Related Commands

prefix-set	Defines a prefix set.

R3.3 Beta Draft—Cisco Confidential Information

suppress-route

To indicate that a given component of an aggregate should be suppressed, use the **suppress-route** command in route-policy configuration mode.

suppress-route

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or value

Command Modes	Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

Use the **suppress-route** command to indicate that a given component of an aggregate should be suppressed, that is, not advertised.

The **suppress-route** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

Task ID	Task ID	Operations
	route-policy	read, write

Examples	In the following example, if the destination is in 10.1.0.0/16, then the route is not advertised:

```
RP/0/RP0/CPU0:router(config)# route-policy check-aggregate
RP/0/RP0/CPU0:router(config-rpl)# if destination in (10.1.0.0/16) then
RP/0/RP0/CPU0:router(config-rpl-if)# suppress-route
RP/0/RP0/CPU0:router(config-rpl-if)# endif
RP/0/RP0/CPU0:router(config-rpl-if)# end-policy
```

R3.3 Beta Draft—Cisco Confidential Information

tag

To match a specific tag value, use the **tag** command in route-policy configuration mode.

tag {**eq** | **ge** | **le** | **is**} {*integer* | *parameter*}

Syntax Description	eq ge le is	Equal to; greater than or equal to; less than or equal to.
	<i>integer</i>	Integer value. Range is 0 to 4294967295.
	<i>parameter</i>	Parameter value.

Defaults	No default behavior or value

Command Modes	Route-policy configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.
	Release 3.3	No modification.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **tag** command as a conditional expression within an **if** statement to match a specific tag value.



Note

For a list of all conditional expressions available within an **if** statement, see the **if** command.

A tag is a 32-bit integer that can be associated with a given route.

The **eq** operator matches either a specific tag value or a parameter value. Its variants **ge** and **le** match a range of tag values that are either greater than or equal to or less than or equal to the supplied value or parameter.

Conditions involving the tag can be accessed only from the redistribution attach point.

Task ID	Task ID	Operations
	route-policy	read, write

Examples

In the following example, if the tag equals 10, then the condition returns true:

```
RP/0/RP0/CPU0:router(config-rpl)# if tag eq 10 then
```

R3.3 Beta Draft—Cisco Confidential Information

unsuppress route

To indicate that a given component of an aggregate should be unsuppressed, use the **unsuppress-route** command in route-policy configuration mode.

unsuppress-route

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or value

Command Modes	Route-policy configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i>.

Use the **unsuppress-route** command to indicate that a given component of an aggregate should be unsuppressed, that is, allowed to be advertised again.

The **unsuppress-route** command can be used as an action statement within an **if** statement. For a list of all action statements available within an **if** statement, see the **if** command.

Task ID	Task ID	Operations
	route-policy	read, write

Examples	In the following example, if the destination is in 10.1.0.0/16, then the route is not advertised:

```
RP/0/RP0/CPU0:router(config)# route-policy check-aggregate
RP/0/RP0/CPU0:router(config-rpl)# if destination in (10.1.0.0/16) then
RP/0/RP0/CPU0:router(config-rpl-if)# unsuppress-route
RP/0/RP0/CPU0:router(config-rpl-if)# endif
RP/0/RP0/CPU0:router(config-rpl-if)# end-policy
```

R3.3 Beta Draft – Cisco Confidential Information

Static Routing Commands on Cisco IOS XR Software

Beta Draft Cisco Confidential Information

This chapter describes the commands used to establish static routes.

For detailed information about static routing concepts, configuration tasks, and examples, see the *Implementing Static Routes on Cisco IOS XR Software* configuration guide.

R3.3 Beta Draft—Cisco Confidential Information**address-family (Static Routes)**

To enter address family configuration modes while configuring static routes, use the **address-family** command in the appropriate configuration mode. To disable support for an address family, use the **no** form of this command.

address-family {**ipv4** | **ipv6**} {**unicast** | **multicast**} [*prefix mask*] [*ip-address* | *interface-type interface-instance*] [**vrf** *vrf-name* {*ip-address* | *interface-type interface-instance*}] [**distance**] [**tag tag**] [**permanent**]

no address-family {**ipv4** | **ipv6**} {**unicast** | **multicast**} [*prefix mask*] [*ip-address* | *interface-type interface-instance*] [**vrf** *vrf-name* {*ip-address* | *interface-type interface-instance*}] [**distance**] [**tag tag**] [**permanent**]

Syntax Description

ipv4	Specifies IP Version 4 address prefixes.
ipv6	Specifies IP Version 6 address prefixes. This option is available only in static router configuration mode.
unicast	Specifies unicast address prefixes.
multicast	Specifies multicast address prefixes. This option is available only in static router configuration mode.
<i>prefix</i>	(Optional) IP route prefix for the destination.
<i>mask</i>	(Optional) Prefix mask for the destination. The network mask can be specified in either of two ways: • The network mask can be a four-part, dotted-decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit is a network address. • The network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are 1s, and the corresponding bits of the address are the network address.
<i>ip-address</i>	(Optional) IP address of the next hop that can be used to reach that network. The IP address is required, not optional, if the interface type and number are not specified. You can specify an IP address and an interface type and interface number.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.

R3.3 Beta Draft—Cisco Confidential Information

<i>interface-instance</i>	(Optional) Either a physical interface instance or a virtual interface instance as follows: - Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0. - Virtual interface instance. Number range varies depending on interface type. For more information about the syntax for the router, use the question mark (?) online help function.
vrf <i>vrf-name</i>	(Optional) Specifies a destination VRF. This option is available when the ipv4 keyword is used. The following names cannot be used: all, default, and global.
<i>distance</i>	(Optional) An administrative distance. Range is 1 to 254.
tag <i>tag</i>	(Optional) Specifies a tag value that can be used as a “match” value for controlling redistribution using route policies. Range is 1 to 4294967295.
permanent	(Optional) Specifies that the route is not removed from the routing table, even if the next-hop interface shuts down or next-hop IP address is not reachable.

Defaults

When entering address family configuration mode from static router configuration mode, all static routes belong to the default VRF.

Command Modes

Static router configuration
VRF static router configuration

Command History

Release	Modification
Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	static	read, write
	bgp, ospf, hsrp, isis, vrrp, multicast, or network	read, write

Examples

The following example shows how to configure an IPv4 unicast address family static route:

```
RP/0/RP0/CPU0:router(config)# router static
RP/0/RP0/CPU0:router(config-static-route)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-vrf-afi-static-route)# 192.168.0.1/24 loopback 5
```

Related Commands

Command	Description
network (BGP)	Specifies a list of networks for the BGP routing process.
show route	Displays the current contents of the routing table.
show route static	Displays the static routes in a routing table.
show route summary	Displays the current contents of the routing table in summary format.
vrf (Static Routes)	Enters VRF static route configuration mode.

R3.3 Beta Draft—Cisco Confidential Information

maximum path (Static)

To change the maximum number of allowable static routes, use the **maximum path** command in static router configuration mode. To remove the **maximum path** command from the configuration file and restore the system to its default condition, use the **no** form of this command.

maximum path {ipv4 | ipv6} *value*

no maximum path {ipv4 | ipv6} *value*

Syntax Description	ipv4 ipv6	Specifies IP Version 4 (IPv4) or IP Version 6 (IPv6) address prefixes.
	<i>value</i>	Maximum number of static routes for the given AFI. The range is 1 to 140000.

Defaults	<i>value</i> : 4000

Command Modes	Static router configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

If you use the **maximum path** command to reduce the configured maximum allowed number of static routes for a given table below the number of static routes currently configured, the change is rejected. In addition, understand the following behavior: If you commit a batch of routes that would, when grouped, push the number of static routes configured above the maximum allowed, the first *n* routes in the batch and the number previously configured are accepted, and the remainder rejected. The *n* argument is the difference between the maximum number allowed and the number previously configured.

Task ID	Task ID	Operations
	static	read, write

Examples	The following example shows how to set the maximum number of static IPv4 routes to 100000:

```
RP/0/RP0/CPU0:router(config-static-route)# maximum path ipv4 100000
```

The following example shows how to remove the preceding configuration and set the maximum number of static IPv4 routes back to the default:

```
RP/0/RP0/CPU0:router(config-static-route)# no maximum path ipv4 100000
```

■ maximum path (Static)

R3.3 Beta Draft – Cisco Confidential Information

Related Commands	Command	Description
	<code>router static</code>	Establishes a static route.
	<code>show route static</code>	Displays the static routes in a routing table.

R3.3 Beta Draft—Cisco Confidential Information

router static

To configure static routes, use the **router static** command in global configuration mode. To remove the all static route configurations, use the **no** form of this command.

router static

no router static

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values

Command Modes	Global configuration

Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .

Task ID	Task ID	Operations
	static	read, write
	bgp, ospf, hsrp, isis, vrrp, multicast, or network	read, write

Examples	The following example shows how to configure static routes:

```
RP/0/RP0/CPU0:router(config)# router static
RP/0/RP0/CPU0:router(config-static-route)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-vrf-afi-static-route)# 192.168.0.1/24 loopback 5
RP/0/RP0/CPU0:router(config-vrf-afi-static-route)# 192.168.0.2/24 10.1.1.1
```

R3.3 Beta Draft—Cisco Confidential Information

vrf (Static Routes)

To configure a VPN routing and forwarding (VRF) instance and enter VRF configuration mode, use the **vrf** command in router configuration mode. To remove the VRF instance from the configuration file and restore the system to its default condition, use the **no** form of this command.

```
vrf vrf-name

no vrf vrf-name
```

Syntax Description	vrf-name Name of the VRF instance. The following names cannot be used: all, default, and global.	
Defaults	No default behavior or values	
Command Modes	Static router configuration	
Command History	Release	Modification
	Release 3.3	This command was introduced on the Cisco CRS-1 and Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **vrf** command to configure a VRF instance. A VRF instance is a collection of VPN routing and forwarding tables maintained at the provider edge (PE) router.

If you are configuring a default VRF route, you do not need to enter VRF configuration mode. For example, routes 192.168.0.1/24 and 192.168.0.2/24 are configured as follows:

```
router static
address ipv4 unicast
  192.168.0.1/24 loopback 5
  192.168.0.2/24 10.1.1.1
```

Routes 192.168.0.1/24 and 192.168.0.2/24 are default VRF routes.

Routes 172.168.40.24/24 and 172.168.40.25/24 are configured as follows:

```
router static
vrf vrf_A
address ipv4 unicast
  172.168.40.24/24 loopback 1
  172.168.40.25/24 vrf default 192.168.0.1/24
```

Routes 172.168.40.24/24 and 172.168.40.25/24 belong to vrf_A. Route 172.168.40.24/24 is not installed in vrf_A until route 192.168.0.1/24 (a default VRF route) is resolved.

R3.3 Beta Draft—Cisco Confidential Information

Task ID	Task ID	Operations
	static	read, write

Examples The following example shows how to configure a VRF instance and enter VRF configuration mode:

```
RP/0/RP0/CPU0:router(config)# router static
RP/0/RP0/CPU0:router(config-static-route)# vrf vrf-1
RP/0/RP0/CPU0:router(config-vrf-static-route)#
```

Related Commands	Command	Description
	address-family (Static Routes)	Enters address family configure mode and allows you to configure a static route.

R3.3 Beta Draft – Cisco Confidential Information

 |

HR	Cisco IOS XR Interface and Hardware Component Command Reference
IR	Cisco IOS XR IP Addresses and Services Command Reference
MCR	Cisco IOS XR Multicast Command Reference
MPR	Cisco IOS XR MPLS Command Reference
QR	Cisco IOS XR Modular Quality of Service Command Reference
RR	Cisco IOS XR Routing Command Reference
SMR	Cisco IOS XR System Management Command Reference
SR	Cisco IOS XR System Security Command Reference

A

abort command [RR-920](#)
add command [RR-921](#)
address-family (BGP) command [RR-2](#)
address-family (IS-IS) command [RR-364](#)
address-family (OSPF) command [RR-538](#)
address-family (OSPFv3) command [RR-702](#)
address-family (Static Routes) [RR-1126](#)
address-family ipv4 (EIGRP) command [RR-294](#)
adjacency-check disable command [RR-366](#)
advertisement-interval command [RR-4](#)
af-group command [RR-6](#)
aggregate-address command [RR-8](#)
allowas-in command [RR-10](#)
apply command [RR-922](#)
area (OSPF) command [RR-539](#)
area (OSPFv3) command [RR-703](#)
as-path in command [RR-924](#)
as-path is-local command [RR-926](#)
as-path length command [RR-928](#)
as-path neighbor-is command [RR-930](#)
as-path originates-from command [RR-932](#)
as-path passes-through command [RR-934](#)
as-path-set command [RR-936](#)
as-path unique-length command [RR-938](#)

authentication (OSPF) command [RR-541](#)
authentication (OSPFv3) command [RR-705](#)
authentication-key (OSPF) command [RR-543](#)
auto-cost (OSPF) command [RR-545](#)
auto-cost (OSPFv3) command [RR-707](#)
autonomous-system command [RR-298](#)
auto-summary (EIGRP) command [RR-296](#)
auto-summary command [RR-866](#)

B

bandwidth-percent (EIGRP) command [RR-299](#)
bgp as-path-loopcheck command [RR-11](#)
bgp attribute-download command [RR-12](#)
bgp auto-policy-soft-reset disable command [RR-13](#)
bgp bestpath as-path ignore command [RR-15](#)
bgp bestpath compare-routerid command [RR-17](#)
bgp bestpath med always command [RR-19](#)
bgp bestpath med confed command [RR-21](#)
bgp bestpath med missing-as-worst command [RR-23](#)
bgp cluster-id command [RR-25](#)
bgp confederation identifier command [RR-27](#)
bgp confederation peers [RR-29](#)
bgp dampening command [RR-31](#)
bgp default local-preference command [RR-33](#)
bgp enforce-first-as disable command [RR-34](#)
bgp fast-external-fallover disable command [RR-36](#)
bgp graceful-restart command [RR-37](#)
bgp graceful-restart graceful-reset command [RR-39](#)
bgp graceful-restart purge-time command [RR-41](#)
bgp graceful-restart restart-time command [RR-43](#)
bgp graceful-restart stalepath-time command [RR-45](#)
bgp log neighbor changes disable command [RR-47](#)
bgp maximum neighbor command [RR-49](#)
bgp redistribute-internal command [RR-50](#)

R3.3 Beta Draft—Cisco Confidential Information

bgp router-id command [RR-52](#)
 bgp scan-time command [RR-54](#)
 bgp update-delay command [RR-56](#)
 bgp write-limit command [RR-58](#)
 broadcast-for-v2 command [RR-868](#)

C

capability opaque command [RR-547](#)
 capability orf prefix command [RR-60](#)
 circuit-type command [RR-368](#)
 clear bgp command [RR-63](#)
 clear bgp dampening command [RR-65](#)
 clear bgp flap-statistics command [RR-67](#)
 clear bgp peer-drops command [RR-69](#)
 clear bgp performance-statistics command [RR-70](#)
 clear bgp self-originated command [RR-71](#)
 clear bgp shutdown command [RR-73](#)
 clear bgp soft command [RR-75](#)
 clear eigrp events command [RR-301](#)
 clear eigrp logging command [RR-302](#)
 clear eigrp neighbors command [RR-303](#)
 clear eigrp topology command [RR-305](#)
 clear isis process command [RR-370](#)
 clear isis route command [RR-372](#)
 clear isis statistics command [RR-374](#)
 clear ospf process command [RR-548](#)
 clear ospf redistribution command [RR-550](#)
 clear ospf routes command [RR-552](#)
 clear ospf statistics command [RR-554](#)
 clear ospfv3 process command [RR-709](#)
 clear ospfv3 redistribution command [RR-710](#)
 clear ospfv3 routes command [RR-711](#)
 clear ospfv3 statistics command [RR-712](#)
 clear rip command [RR-869](#)
 clear rip database command [RR-870](#)
 clear rip interface command [RR-872](#)
 clear rip out-of-memory command [RR-873](#)
 clear rip statistics command [RR-875](#)

clear route command [RR-836](#)
 community is-empty command [RR-940](#)
 community matches-any command [RR-941](#)
 community matches-every command [RR-943](#)
 community-set command [RR-945](#)
 cost (OSPF) command [RR-556](#)
 cost (OSPFv3) command [RR-714](#)
 csnp-interval command [RR-376](#)

D

database-filter all out (OSPF) command [RR-558](#)
 database-filter all out (OSPFv3) command [RR-716](#)
 dead-interval (OSPF) command [RR-560](#)
 dead-interval (OSPFv3) command [RR-718](#)
 default-cost (OSPF) command [RR-562](#)
 default-cost (OSPFv3) command [RR-720](#)
 default-information command [RR-307](#)
 default-information originate (RIP) command [RR-877](#)
 default-information originate (BGP) command [RR-78](#)
 default-information originate (IS-IS) command [RR-378](#)
 default-information originate (OSPF) command [RR-564](#)
 default-information originate (OSPFv3) command [RR-722](#)
 default-metric (BGP) command [RR-80](#)
 default-metric (EIGRP) command [RR-308](#)
 default-metric (OSPF) command [RR-566](#)
 default-metric (OSPFv3) command [RR-724](#)
 default-metric (RIP) command [RR-878](#)
 default-originate command [RR-81](#)
 delete community command [RR-947](#)
 delete extcommunity command [RR-949](#)
 demand-circuit (OSPF) command [RR-568](#)
 demand-circuit (OSPFv3) command [RR-726](#)
 description (BGP) command [RR-83](#)
 destination in command [RR-951](#)
 disable (IS-IS) command [RR-380](#)
 disable-dn-bit-check command [RR-570](#)
 distance (EIGRP) command [RR-310](#)
 distance (ISIS) command [RR-381](#)

R3.3 Beta Draft—Cisco Confidential Information

distance admin-distance (RIP) command [RR-880](#)
 distance bgp command [RR-84](#)
 distance ospf command [RR-573](#)
 distance ospfv3 command [RR-728](#)
 distribute-list command [RR-575](#)
 distribute-list prefix-list in command [RR-730](#)
 distribute-list prefix-list out command [RR-732](#)
 dmz-link-bandwidth command [RR-86](#)
 domain-id command [RR-577](#)
 domain-tag command [RR-578](#)
 drop command [RR-953](#)

E

ebgp-multihop command [RR-88](#)
 edit command [RR-955](#)
 EIGRP (Enhanced IGRP)
 interfaces, displaying [RR-341](#)
 end-policy command [RR-957](#)
 end-set command [RR-958](#)
 export route-policy command [RR-90](#)
 export route-target command [RR-91](#)
 extcommunity rt is-empty command [RR-959](#)
 extcommunity rt matches-any command [RR-960](#)
 extcommunity rt matches-every command [RR-962](#)
 extcommunity-set command [RR-964](#)
 extcommunity-set cost command [RR-966](#)
 extcommunity-set rt command [RR-967](#)
 extcommunity-set soo command [RR-968](#)
 ext-community soo matches-any command [RR-970](#)
 ext-community soo matches-every command [RR-972](#)
 ext-community sso is-empty command [RR-969](#)

F

flood-reduction (OSPF) command [RR-579](#)
 flood-reduction (OSPFv3) command [RR-734](#)

G

graceful-restart (OSPFv3) command [RR-736](#)

H

hello-interval (EIGRP) command [RR-312](#)
 hello-interval (IS-IS) command [RR-383](#)
 hello-interval (OSPF) command [RR-581](#)
 hello-interval (OSPFv3) command [RR-738](#)
 hello-multiplier command [RR-385](#)
 hello-padding command [RR-387](#)
 hello-password accept command [RR-391](#)
 hello-password command [RR-389](#)
 hold-time (EIGRP) command [RR-313](#)
 hostname dynamic disable command [RR-393](#)

I

if command [RR-974](#)
 ignore lsa mospf command [RR-583](#)
 ignore-lsp-errors command [RR-395](#)
 import route-policy command [RR-93](#)
 import route-target command [RR-94](#)
 instance command [RR-740](#)
 interface (IS-IS) command [RR-397](#)
 interface (OSPF) command [RR-584](#)
 interface (OSPFv3) command [RR-742](#)
 interface (RIP) command [RR-882](#)
 ispf command [RR-399](#)
 ispf startup-delay command [RR-400](#)
 is-type command [RR-400](#)

L

label-allocation-mode command [RR-96](#)
 local-as command [RR-97](#)
 log adjacency changes (IS-IS) command [RR-402](#)

R3.3 Beta Draft—Cisco Confidential Information

log adjacency changes (OSPF) command [RR-586](#)
 log adjacency changes (OSPFv3) command [RR-744](#)
 log-neighbor-changes command [RR-317](#)
 log-neighbor-warnings command [RR-318](#)
 log pdu drops command [RR-404](#)
 lsp-gen-interval command [RR-405](#)
 lsp-interval command [RR-407](#)
 lsp-mtu command [RR-409](#)
 lsp-password accept command [RR-413](#)
 lsp-password command [RR-411](#)
 lsp-refresh-interval command [RR-415](#)

M

maximum interfaces (OSPF) command [RR-589](#)
 maximum interfaces (OSPFv3) command [RR-745](#)
 maximum path (Static) command [RR-1129](#)
 maximum-paths (BGP) command [RR-99](#)
 maximum-paths (EIGRP) command [RR-319](#)
 maximum-paths (IS-IS) command [RR-417](#)
 maximum-paths (OSPF) command [RR-591](#)
 maximum paths (OSPFv3) command [RR-746](#)
 maximum-paths (RIP) command [RR-884](#)
 maximum-prefix (BGP) command [RR-101](#)
 maximum-prefix (EIGRP) command [RR-320](#)
 maximum prefix (RIB) command [RR-838](#)
 maximum-redistributed-prefixes (IS-IS)
 command [RR-418](#)
 maximum redistributed-prefixes (OSPF)
 command [RR-592](#)
 maximum redistributed-prefixes (OSPFv3)
 command [RR-747](#)
 max-lsp-lifetime command [RR-419](#)
 max-metric command [RR-587](#)
 med command [RR-979](#)
 mesh-group (IS-IS) command [RR-421](#)
 message-digest-key command [RR-594](#)
 metric command [RR-423](#)
 metric holddown command [RR-322](#)

metric maximum-hops command [RR-324](#)
 metric-style narrow command [RR-425](#)
 metric-style transition command [RR-427](#)
 metric-style wide command [RR-429](#)
 metric weights command [RR-326](#)
 metric-zero-accept command [RR-885](#)
 mpls ldp sync (OSPF) command [RR-597](#)
 mpls traffic-eng area (OSPF) command [RR-598](#)
 mpls traffic-eng command [RR-433](#)
 mpls traffic-eng router-id (IS-IS) command [RR-435](#)
 mpls traffic-eng router-id (OSPF) command [RR-600](#)
 mtu-ignore (OSPF) command [RR-602](#)
 mtu-ignore (OSPFv3) command [RR-749](#)

N

neighbor (BGP) command [RR-103](#)
 neighbor (OSPF) command [RR-604](#)
 neighbor (OSPFv3) command [RR-751](#)
 neighbor (RIP) command [RR-886](#)
 neighbor database-filter all out command [RR-606](#)
 neighbor-group command [RR-105](#)
 neighbor maximum-prefix command [RR-328](#)
 net command [RR-437](#)
 network (BGP) command [RR-107](#)
 network (OSPF) command [RR-608](#)
 network (OSPFv3) command [RR-753](#)
 network backdoor command [RR-109](#)
 next-hop in command [RR-981](#)
 next-hop-self command [RR-111](#)
 next-hop-self disable command [RR-331](#)
 nsf (IS-IS) command [RR-439](#)
 nsf (OSPF) command [RR-610](#)
 nsf (RIP) command [RR-888](#)
 nsf interface-expires command [RR-441](#)
 nsf interface-timer command [RR-443](#)
 nsf interval (OSPF) command [RR-612](#)
 nsf lifetime (IS-IS) command [RR-445](#)
 nsf lifetime (OSPF) command [RR-613](#)

R3.3 Beta Draft—Cisco Confidential Information

nssa (OSPF) command [RR-614](#)
 nssa (OSPFv3) command [RR-755](#)

O

origin is command [RR-983](#)
 ospf name-lookup command [RR-616](#)
 ospfv3 name-lookup command [RR-757](#)
 output-delay command [RR-889](#)

P

packet-size command [RR-617](#)
 pass command [RR-985](#)
 passive (IS-IS) command [RR-447](#)
 passive (OSPF) command [RR-619](#)
 passive (OSPFv3) command [RR-758](#)
 passive-interface (EIGRP) command [RR-332](#)
 passive-interface (RIP) command [RR-890](#)
 password command [RR-115](#)
 password-disable command [RR-117](#)
 point-to-point command [RR-448](#)
 poison-reverse disable command [RR-892](#)
 prefix-set command [RR-987](#)
 prepend as-path command [RR-989](#)
 priority (IS-IS) command [RR-449](#)
 priority (OSPF) command [RR-621](#)
 priority (OSPFv3) command [RR-760](#)
 propagate level command [RR-451](#)
 protocol command [RR-991](#)

R

range (OSPF) command [RR-623](#)
 range (OSPFv3) command [RR-762](#)
 rd command [RR-119](#)
 rd in command [RR-993](#)
 rd-set command [RR-994](#)

receive-buffer-size command [RR-121](#)
 receive version command [RR-894](#)
 redistribute (BGP) command [RR-123](#)
 redistribute (EIGRP) command [RR-333](#)
 redistribute (IS-IS) command [RR-453](#)
 redistribute (OSPF) command [RR-625](#)
 redistribute (OSPFv3) command [RR-764](#)
 redistribute (RIP) command [RR-895](#)
 redistribute maximum-prefix command [RR-335](#)
 remote-as (BGP) command [RR-127](#)
 remove-private-as command [RR-129](#)
 retain route-target command [RR-131](#)
 retransmit-interval (IS-IS) command [RR-456](#)
 retransmit-interval (OSPF) command [RR-629](#)
 retransmit-interval (OSPFv3) command [RR-768](#)
 retransmit-throttle-interval command [RR-458](#)
 rib-has-route command [RR-996](#)
 route-policy (BGP) command [RR-133](#)
 route-policy (EIGRP) command [RR-337](#)
 route-policy (RIP) command [RR-899](#)
 route-policy (RPL) command [RR-997](#)
 router bgp command [RR-137](#)
 route-reflector-client [RR-135](#)
 router eigrp command [RR-338](#)
 router-id (EIGRP) command [RR-339](#)
 router-id (OSPF) command [RR-631](#)
 router-id (OSPFv3) command [RR-770](#)
 router isis command [RR-460](#)
 router ospf command [RR-633](#)
 router ospfv3 command [RR-772](#)
 router rip command [RR-898](#)
 router static command [RR-1131](#)
 route-type is command [RR-999](#)
 rpl maximum command [RR-1001](#)

S

send-buffer-size command [RR-138](#)
 send-community-ebgp command [RR-140](#)

R3.3 Beta Draft—Cisco Confidential Information

- send-extended-community-ebgp command [RR-142](#)
- send version command [RR-901](#)
- session-group command [RR-144](#)
- session-open-mode command [RR-146](#)
- set-attached-bit command [RR-462](#)
- set community command [RR-1003](#)
- set cost command [RR-1005](#)
- set dampening command [RR-1006](#)
- set eigrp-metric command [RR-1008](#)
- set extcommunity command [RR-1010](#)
- set level command [RR-1012](#)
- set local-preference command [RR-1013](#)
- set med command [RR-1015](#)
- set metric command [RR-1017](#)
- set metric-type (IS-IS) command [RR-1018](#)
- set metric-type (OSPF) command [RR-1019](#)
- set next-hop command [RR-1021](#)
- set origin command [RR-1023](#)
- set-overload-bit command [RR-464](#)
- set rip-metric command [RR-1024](#)
- set tag command [RR-1025](#)
- set traffic-index command [RR-1026](#)
- set weight command [RR-1028](#)
- show bgp advertised command [RR-155](#)
- show bgp af-group command [RR-161](#)
- show bgp attribute-key command [RR-164](#)
- show bgp cidr-only command [RR-168](#)
- show bgp command [RR-148](#)
- show bgp community command [RR-172](#)
- show bgp convergence command [RR-176](#)
- show bgp count-only command [RR-179](#)
- show bgp dampened-paths command [RR-183](#)
- show bgp flap-statistics command [RR-187](#)
- show bgp inconsistent-as command [RR-192](#)
- show bgp neighbor-group command [RR-196](#)
- show bgp neighbors command [RR-200](#)
- show bgp paths command [RR-214](#)
- show bgp policy command [RR-216](#)
- show bgp process command [RR-223](#)
- show bgp regexp command [RR-238](#)
- show bgp route-policy command [RR-242](#)
- show bgp session-group command [RR-246](#)
- show bgp summary command [RR-249](#)
- show bgp truncated-communities command [RR-253](#)
- show bgp update-group command [RR-257](#)
- show bgp vrf imported-routes command [RR-262](#)
- show eigrp accounting command [RR-340](#)
- show eigrp interfaces command [RR-341](#)
- show eigrp topology command [RR-345](#)
- show eigrp traffic command [RR-347](#)
- show isis adjacency command [RR-466](#)
- show isis adjacency-log command [RR-469](#)
- show isis checkpoint adjacency command [RR-471](#)
- show isis checkpoint interface command [RR-473](#)
- show isis checkpoint lsp command [RR-475](#)
- show isis database command [RR-477](#)
- show isis database-log command [RR-484](#)
- show isis hostname command [RR-486](#)
- show isis interface command [RR-488](#)
- show isis lsp-log command [RR-492](#)
- show isis mesh-group command [RR-495](#)
- show isis mpls traffic-eng adjacency-log command [RR-497](#)
- show isis mpls traffic-eng advertisements command [RR-499](#)
- show isis mpls traffic-eng tunnel command [RR-502](#)
- show isis neighbors command [RR-504](#)
- show isis protocol command [RR-507](#)
- show isis route command [RR-509](#)
- show isis spf-log command [RR-511](#)
- show isis statistics command [RR-517](#)
- show isis topology command [RR-521](#)
- show ospf border-routers command [RR-638](#)
- show ospf command [RR-635](#)
- show ospf database command [RR-640](#)
- show ospf flood-list command [RR-651](#)
- show ospf interface command [RR-653](#)
- show ospf mpls traffic-eng command [RR-656](#)

R3.3 Beta Draft—Cisco Confidential Information

- show ospf neighbor command [RR-661](#)
- show ospf request-list command [RR-667](#)
- show ospf retransmission-list command [RR-670](#)
- show ospf route command [RR-672](#)
- show ospf summary-prefix command [RR-676](#)
- show ospfv3 border-routers command [RR-777](#)
- show ospfv3 command [RR-774](#)
- show ospfv3 database command [RR-779](#)
- show ospfv3 flood-list command [RR-790](#)
- show ospfv3 interface command [RR-793](#)
- show ospfv3 neighbor command [RR-796](#)
- show ospfv3 retransmission-list command [RR-805](#)
- show ospfv3 route command [RR-807](#)
- show ospfv3 summary-prefix command [RR-809](#)
- show ospfv3 virtual-links command [RR-811](#)
- show ospf virtual-links command [RR-678](#)
- show ospv3 request-list command [RR-802](#)
- show protocols (BGP) command [RR-264](#)
- show protocols (IS-IS) command [RR-524](#)
- show protocols (OSPF) command [RR-680](#)
- show protocols (OSPFv3) command [RR-813](#)
- show rip command [RR-902](#)
- show rip database command [RR-904](#)
- show rip interface command [RR-906](#)
- show rip statistics command [RR-908](#)
- show route command [RR-841](#)
- show route connected command [RR-850](#)
- show route local command [RR-852](#)
- show route longer-prefixes command [RR-854](#)
- show route static command [RR-858](#)
- show route summary command [RR-860](#)
- show route vrf command [RR-862](#)
- show rpl active as-path-set command [RR-1030](#)
- show rpl active community-set command [RR-1033](#)
- show rpl active extcommunity-set command [RR-1036](#)
- show rpl active prefix-set command [RR-1041](#)
- show rpl active route-policy command [RR-1039](#)
- show rpl as-path-set attachpoints command [RR-1046](#)
- show rpl as-path-set command [RR-1044](#)
- show rpl as-path-set references command [RR-1049](#)
- show rpl community-set attachpoints command [RR-1054](#)
- show rpl community-set command [RR-1052](#)
- show rpl community-set references command [RR-1056](#)
- show rpl extcommunity-set attachpoints command [RR-1061](#)
- show rpl extcommunity-set command [RR-1059](#)
- show rpl extcommunity-set references command [RR-1064](#)
- show rpl inactive as-path-set command [RR-1067](#)
- show rpl inactive community-set command [RR-1070](#)
- show rpl inactive extcommunity-set command [RR-1073](#)
- show rpl inactive prefix-set command [RR-1076](#)
- show rpl inactive route-policy command [RR-1079](#)
- show rpl maximum command [RR-1082](#)
- show rpl prefix-set attachpoints command [RR-1086](#)
- show rpl prefix-set command [RR-1084](#)
- show rpl prefix-set references command [RR-1089](#)
- show rpl route-policy attachpoints command [RR-1095](#)
- show rpl route-policy command [RR-1092](#)
- show rpl route-policy references command [RR-1098](#)
- show rpl route-policy uses command [RR-1101](#)
- show rpl unused as-path-set command [RR-1104](#)
- show rpl unused community-set command [RR-1107](#)
- show rpl unused extcommunity-set command [RR-1110](#)
- show rpl unused prefix-set command [RR-1113](#)
- show rpl unused route-policy command [RR-1116](#)
- shutdown (BGP) command [RR-266](#)
- shutdown (IS-IS) command [RR-527](#)
- single-topology command [RR-528](#)
- site-of-origin (EIGRP) command [RR-348](#)
- site-of-origin (RIP) command [RR-909](#)
- socket-receive-buffer-size command [RR-268](#)
- socket send-buffer-size command [RR-270](#)
- soft-reconfiguration inbound command [RR-272](#)
- source in command [RR-1119](#)
- spf-interval command [RR-530](#)
- split-horizon disable (EIGRP) command [RR-349](#)
- split-horizon disable (RIP) command [RR-911](#)
- stub (EIGRP) command [RR-350](#)

R3.3 Beta Draft—Cisco Confidential Information

stub (OSPF) command [RR-683](#)
 stub (OSPFv3) command [RR-815](#)
 summary-address (EIGRP) command [RR-352](#)
 summary-prefix (IS-IS) command [RR-532](#)
 summary-prefix (OSPF) command [RR-685](#)
 summary-prefix (OSPFv3) command [RR-817](#)
 suppressed (IS-IS) command [RR-534](#)
 suppress-route command [RR-1121](#)

T

table-policy command [RR-275](#)
 tag command [RR-1122](#)
 timers (BGP) command [RR-277](#)
 timers active-time command [RR-354](#)
 timers basic command [RR-913](#)
 timers bgp command [RR-279](#)
 timers lsa arrival command [RR-819](#)
 timers lsa group-pacing command [RR-687](#)
 timers lsa min-arrival command [RR-689](#)
 timers nsf route-hold (EIGRP) command [RR-356](#)
 timers pacing flood command [RR-821](#)
 timers pacing lsa-group command [RR-823](#)
 timers pacing retransmission command [RR-825](#)
 timers throttle lsa all (OSPF) command [RR-690](#)
 timers throttle lsa-all (OSPFv3) command [RR-827](#)
 timers throttle spf (OSPF) command [RR-692](#)
 timers throttle spf (OSPFv3) command [RR-829](#)
 transmit-delay (OSPF) command [RR-694](#)
 transmit-delay (OSPFv3) command [RR-831](#)
 ttl-security command [RR-281](#)

U

unsuppress route command [RR-1123](#)
 update-source command [RR-284](#)
 use command [RR-286](#)

V

validate-update-source disable command [RR-915](#)
 variance command [RR-358](#)
 virtual-link (OSPF) command [RR-696](#)
 virtual-link (OSPFv3) command [RR-833](#)
 vrf (BGP) command [RR-290](#)
 vrf (EIGRP) command [RR-360](#)
 vrf (OSPF) command [RR-698](#)
 vrf (RIP) command [RR-916](#)
 vrf (Static Routes) command [RR-1132](#)

W

weight command [RR-291](#)