



Cisco IOS IPv6 Command Reference

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



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.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, 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 Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0304R)

Cisco IOS IPv6 Command Reference

Copyright © 2002-2003, Cisco Systems, Inc. All rights reserved.



Introduction IPv6R-1

Cisco IOS IPv6 Commands IPv6R-12



Introduction

This book describes the commands used to configure and monitor IPv6. The commands in this book are organized alphabetically. The following section provides a high-level structure of commands organized by module. All commands within each section are cross-referenced to the corresponding command reference pages in this book.

- ADSL and Deploying Dial Access for IPv6, page 1
- Basic Connectivity for IPv6, page 2
- IPv6 Multicast, page 4
- IPv6 over MPLS, page 6
- IS-IS for IPv6, page 6
- Managing Cisco IOS Applications over IPv6, page 6
- Multiprotocol BGP for IPv6, page 7
- NAT-PT for IPv6, page 7
- OSPF for IPv6, page 8
- QoS for IPv6, page 9
- RIP for IPv6, page 9
- Security for IPv6, page 10
- Static Routes for IPv6, page 10
- Tunneling for IPv6, page 10

For IPv6 configuration tasks and examples, refer to *Implementing IPv6 for Cisco IOS, Release 12.3*.

ADSL and Deploying Dial Access for IPv6

Use the following commands to configure and monitor ADSL and dial access for IPv6:

- debug ipv6 pool
- dialer-list protocol
- ipv6 local pool
- peer default ipv6 address pool
- show ipv6 local pool

Basic Connectivity for IPv6

Use the following commands to configure and monitor basic functions for IPv6:

- atm route-bridge
- clear ipv6 dhcp binding
- clear ipv6 dhcp client
- clear ipv6 neighbors
- clear ipv6 route
- clear ipv6 traffic
- copy
- debug ipv6 cef drop
- debug ipv6 cef events
- debug ipv6 cef hash
- debug ipv6 cef receive
- debug ipv6 cef table
- debug ipv6 dhcp
- debug ipv6 dhcp database
- debug ipv6 icmp
- debug ipv6 nd
- debug ipv6 packet
- debug ipv6 routing
- dns-server (IPv6)
- domain-name (IPv6)
- frame-relay map ipv6
- ip name-server
- ipv6 address
- ipv6 address anycast
- ipv6 address autoconfig
- ipv6 address eui-64
- ipv6 address link-local
- ipv6 atm-vc
- ipv6 cef
- ipv6 cef accounting
- ipv6 cef distributed
- ipv6 dhcp client pd
- ipv6 dhcp database
- ipv6 dhcp pool
- ipv6 dhcp server

- ipv6 enable
- ipv6 general-prefix
- ipv6 hop-limit
- ipv6 icmp error-interval
- ipv6 mtu
- ipv6 nd dad attempts
- ipv6 nd managed-config-flag
- ipv6 nd ns-interval
- ipv6 nd other-config-flag
- ipv6 nd prefix
- ipv6 nd prefix-advertisement
- ipv6 nd ra-interval
- ipv6 nd ra-lifetime
- ipv6 nd reachable-time
- ipv6 nd suppress-ra
- ipv6 neighbor
- ipv6 redirects
- ipv6 unicast-routing
- ipv6 unnumbered
- ipv6 verify unicast reverse-path
- neighbor activate
- neighbor override-capability-neg
- neighbor send-label
- neighbor translate-update
- neighbor update-source
- ping
- ping ipv6
- prefix-delegation
- prefix-delegation pool
- protocol ipv6 (ATM)
- show atm map
- show cdp entry
- show cdp neighbors
- show cef
- show cef interface
- show cef linecard
- show frame-relay map
- show ipv6 cef

- show ipv6 cef adjacency
- show ipv6 cef non-recursive
- show ipv6 cef summary
- show ipv6 cef traffic prefix-length
- show ipv6 cef unresolved
- show ipv6 dhcp
- show ipv6 dhcp binding
- show ipv6 dhcp database
- show ipv6 dhcp interface
- show ipv6 dhcp pool
- show ipv6 general-prefix
- show ipv6 interface
- show ipv6 mtu
- show ipv6 neighbors

IPv6 Multicast

Use the following commands to configure and monitor multicast for IPv6:

- clear ipv6 mfib counters
- clear ipv6 mld counters
- clear ipv6 mld traffic
- clear ipv6 pim counters
- clear ipv6 pim reset
- clear ipv6 pim topology
- debug ipv6 mfib
- debug ipv6 mld
- debug ipv6 mrrib client
- debug ipv6 mrrib io
- debug ipv6 mrrib proxy
- debug ipv6 mrrib route
- debug ipv6 mrrib table
- debug ipv6 pim
- ipv6 mfib
- ipv6 mfib fast
- ipv6 mfib-mode centralized-only
- ipv6 mld access-group
- ipv6 mld join-group
- ipv6 mld query-interval

- ipv6 mld query-max-response-time
- ipv6 mld query-timeout
- ipv6 mld router
- ipv6 mld static-group
- ipv6 multicast-routing
- ipv6 pim
- ipv6 pim accept-register
- ipv6 pim dr-priority
- ipv6 pim hello-interval
- ipv6 pim join-prune-interval
- show ipv6 pim join-prune statistic
- ipv6 pim rp embedded
- ipv6 pim rp-address
- ipv6 pim spt-threshold infinity
- show ipv6 mfib
- show ipv6 mfib active
- show ipv6 mfib count
- show ipv6 mfib interface
- show ipv6 mfib status
- show ipv6 mfib summary
- show ipv6 mld groups summary
- show ipv6 mld interface
- show ipv6 mld traffic
- show ipv6 mrib client
- show ipv6 mrib route
- show ipv6 mroute
- show ipv6 mroute active
- show ipv6 pim bsr
- show ipv6 pim group-map
- show ipv6 pim interface
- show ipv6 pim join-prune statistic
- show ipv6 pim neighbor
- show ipv6 pim range-list
- show ipv6 pim topology
- show ipv6 pim traffic
- show ipv6 pim tunnel
- show ipv6 rpf

IPv6 over MPLS

Use the following commands to configure and monitor MPLS for IPv6:

- `mpls ipv6 source-interface`
- `show mpls forwarding-table`

IS-IS for IPv6

Use the following commands to configure and monitor IS-IS for IPv6:

- `address-family ipv6 (IS-IS)`
- `adjacency-check`
- `debug isis spf-events`
- `default-information originate (IPv6 IS-IS)`
- `distance (IPv6)`
- `ipv6 router isis`
- `isis ipv6 metric`
- `multi-topology`
- `prc-interval (IPv6)`
- `show clns neighbors`
- `show ipv6 protocols`
- `show isis database`
- `show isis ipv6 rib`
- `show isis spf-log`
- `show isis topology`
- `spf-interval (IPv6)`
- `summary-prefix (IPv6 IS-IS)`

Managing Cisco IOS Applications over IPv6

Use the following commands to configure and manage Cisco IOS applications over IPv6:

- `ipv6 host`
- `show ip sockets`
- `show ipv6 routers`
- `show ipv6 traffic`
- `ssh`
- `telnet`
- `traceroute`

Multiprotocol BGP for IPv6

Use the following commands to configure and monitor multiprotocol BGP for IPv6:

- address-family ipv6
- clear bgp ipv6
- clear bgp ipv6 dampening
- clear bgp ipv6 external
- clear bgp ipv6 flap-statistics
- clear bgp ipv6 peer-group
- debug bgp ipv6 dampening
- debug bgp ipv6 updates
- distance bgp (IPv6)
- maximum-paths (IPv6)
- redistribute (IPv6)
- set ipv6 next-hop (BGP)
- show bgp ipv6
- show bgp ipv6 community
- show bgp ipv6 community-list
- show bgp ipv6 dampened-paths
- show bgp ipv6 filter-list
- show bgp ipv6 flap-statistics
- show bgp ipv6 inconsistent-as
- show bgp ipv6 labels
- show bgp ipv6 neighbors
- show bgp ipv6 paths
- show bgp ipv6 peer-group
- show bgp ipv6 prefix-list
- show bgp ipv6 quote-regexp
- show bgp ipv6 regexp
- show bgp ipv6 route-map
- show bgp ipv6 summary
- synchronization (IPv6)

NAT-PT for IPv6

Use the following commands to configure and monitor NAT-PT for IPv6:

- clear ipv6 nat translation
- debug ipv6 nat

- ipv6 nat
- ipv6 nat max-entries
- ipv6 nat prefix
- ipv6 nat translation
- ipv6 nat v4v6 pool
- ipv6 nat v4v6 source
- ipv6 nat v6v4 pool
- ipv6 nat v6v4 source
- show ipv6 nat statistics
- show ipv6 nat translations

OSPF for IPv6

Use the following commands to configure and monitor OSPF for IPv6:

- area authentication (IPv6)
- area range
- area virtual-link
- clear ipv6 ospf
- debug ipv6 ospf
- debug ipv6 ospf events
- debug ipv6 ospf lsdb
- debug ipv6 ospf packet
- debug ipv6 ospf spf statistic
- ipv6 ospf area
- ipv6 ospf authentication
- ipv6 ospf cost
- ipv6 ospf database-filter all out
- ipv6 ospf dead-interval
- ipv6 ospf demand-circuit
- ipv6 ospf flood-reduction
- ipv6 ospf hello-interval
- ipv6 ospf mtu-ignore
- ipv6 ospf name-lookup
- ipv6 ospf neighbor
- ipv6 ospf network
- ipv6 ospf priority
- ipv6 ospf retransmit-interval
- ipv6 ospf transmit-delay

- ipv6 router ospf
- show ipv6 ospf
- show ipv6 ospf border-routers
- show ipv6 ospf database
- show ipv6 ospf flood-list
- show ipv6 ospf interface
- show ipv6 ospf neighbor
- show ipv6 ospf request-list
- show ipv6 ospf retransmission-list
- show ipv6 ospf summary-prefix
- show ipv6 ospf virtual-links
- summary-prefix (IPv6 OSPF)

QoS for IPv6

Use the following commands to configure and monitor QoS for IPv6:

- match dscp
- match precedence
- match protocol
- set dscp
- set precedence

RIP for IPv6

Use the following commands to configure and monitor RIP for IPv6:

- clear ipv6 rip
- debug ipv6 rip
- distribute-list prefix-list (IPv6 RIP)
- ipv6 rip default-information
- ipv6 rip enable
- ipv6 rip metric-offset
- ipv6 rip summary-address
- ipv6 router rip
- match ipv6 address
- match ipv6 next-hop
- match ipv6 route-source
- poison-reverse (IPv6 RIP)
- port (IPv6 RIP)

- show ipv6 rip
- split-horizon (IPv6 RIP)
- timers (IPv6 RIP)

Security for IPv6

Use the following commands to configure and monitor security for IPv6:

- clear ipv6 access-list
- clear ipv6 prefix-list
- debug crypto ipv6 ipsec
- debug crypto ipv6 packet
- deny (IPv6)
- evaluate (IPv6)
- ipv6 access-class
- ipv6 access-list
- ipv6 access-list log-update threshold
- ipv6 prefix-list
- ipv6 prefix-list sequence-number
- ipv6 traffic-filter
- permit (IPv6)
- remark (IPv6)
- show crypto ipsec policy
- show crypto ipsec sa ipv6
- show ipv6 access-list
- show ipv6 prefix-list

Static Routes for IPv6

Use the following commands to configure and monitor static routes for IPv6:

- ipv6 route
- show ipv6 route
- show ipv6 route summary
- show ipv6 static

Tunneling for IPv6

Use the following commands to configure and monitor tunneling for IPv6:

- show ipv6 tunnel

- tunnel mode ipv6ip



Cisco IOS IPv6 Commands

address-family ipv6

To enter address family configuration mode for configuring routing sessions such as Border Gateway Protocol (BGP) that use standard IPv6 address prefixes, use the **address-family ipv6** command in router configuration mode. To disable address family configuration mode, use the **no** form of this command.

address-family ipv6 [unicast | multicast]

no address-family ipv6 [unicast | multicast]

Syntax Description

| | |
|------------------|---|
| unicast | (Optional) Specifies IPv6 unicast address prefixes. |
| multicast | (Optional) Specifies IPv6 multicast address prefixes. |

Defaults

IPv6 address prefixes are not enabled. Unicast address prefixes are the default when IPv6 address prefixes are configured.



Note

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

Command Modes

Router configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.0(26)S | The multicast keyword was added. |
| 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines

The **address-family ipv6** command places the router in address family configuration mode (prompt: config-router-af), from which you can configure routing sessions that use standard IPv6 address prefixes.

Within address family configuration mode, use the question mark (?) online help function to display supported commands. The BGP commands supported in address family configuration mode configure the same functionality as the BGP commands supported in router configuration mode; however, the BGP commands in router configuration mode configure functionality only for the IPv4 unicast address prefix. To configure BGP commands and functionality for other address family prefixes (for example, the IPv4 multicast or IPv6 unicast address prefixes), you must enter address family configuration mode for those address prefixes using the **address-family ipv4** command or the **address-family ipv6** command.

Use the **multicast** keyword to specify an administrative distance for multicast BGP routes to be used in reverse path forwarding (RPF) lookups.

Examples

The following example places the router in address family configuration mode and specifies unicast address prefixes for the IPv6 address family:

```
Router(config)# router bgp 100  
Router(config-router)# address-family ipv6 unicast  
Router(config-router-af)#
```

The following example places the router in address family configuration mode and specifies multicast address prefixes for the IPv6 address family:

```
Router(config)# router bgp 100  
Router(config-router)# address-family ipv6 multicast  
Router(config-router-af)#
```

Related Commands

| Command | Description |
|-------------------------------------|---|
| address-family ipv4 | Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv4 address prefixes. |
| address-family vpnv4 | Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes. |
| bgp default ipv4-unicast | Enables the IPv4 unicast address family on all neighbors. |
| neighbor activate | Enables the exchange of information with a BGP neighboring router. |

address-family ipv6 (IS-IS)

To enter address family configuration mode for configuring Intermediate System-to-Intermediate System (IS-IS) routing sessions that use standard IPv6 address prefixes, use the **address-family ipv6** command in router configuration mode. To reset all IPv6-specific global configuration values to their default values, use the **no** form of this command.

address-family ipv6 [unicast]

no address-family ipv6 [unicast]

Syntax Description

| | |
|----------------|---|
| unicast | (Optional) Specifies IPv6 unicast address prefixes. |
|----------------|---|

Defaults

IPv6 address prefixes are not enabled. Unicast address prefixes are the default when IPv6 address prefixes are configured.

Command Modes

Router configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(8)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **address-family ipv6** command places the router in address family configuration mode (prompt: config-router-af), from which you can configure IPv6-specific settings. To leave address family configuration mode and return to router configuration mode, enter the **exit-address-family** command.

Within address family configuration mode, use the question mark (?) online help function to display supported commands. Many of the IS-IS commands supported in address family configuration mode are identical in syntax to IS-IS commands supported in router configuration mode. Note that commands issued in address family configuration mode apply to IPv6 only, while the matching commands in router configuration mode are IPv4-specific.

Examples

The following example places the router in address family configuration mode for IS-IS and specifies unicast address prefixes for the IPv6 address family:

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6 unicast
Router(config-router-af)#
```

adjacency-check

To allow Intermediate System-to-Intermediate System (IS-IS) IPv6 or IPv4 protocol-support consistency checks performed on hello packets, use the **adjacency-check** command in address family configuration or router configuration mode. To disable consistency checks on hello packets, use the **no** form of this command.

adjacency-check

no adjacency-check

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Address family configuration
Router configuration

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.2(8)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| | 12.2(15)T | Support was added for router configuration mode. |
| | 12.2(18)S | Support was added for router configuration mode. |
| | 12.0(26)S | Support was added for router configuration mode. |

Usage Guidelines IS-IS performs consistency checks on hello packets and will form an adjacency only with a neighboring router that supports the same set of protocols. A router running IS-IS for both IPv4 and IPv6 will not form an adjacency with a router running IS-IS for IPv4 only.

Use the **no adjacency-check** command in address-family configuration mode 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 will never form an adjacency between a router running IPv4 IS-IS only and a router running IPv6 only.

Use the **no adjacency-check** command in router configuration mode to suppress the IPv4 subnet consistency check and allow IS-IS to form an adjacency with other routers regardless of whether or not they have an IPv4 subnet in common. By default, IS-IS makes checks in hello packets for IPv4 address subnet matching with a neighbor. In multitopology mode, the IPv4 subnet consistency check is automatically suppressed.



Use the **debug isis adjacency packets** command in EXEC mode to check for adjacency errors. Error messages in the output may indicate where routers are failing to establish adjacencies.

Examples

In the following example, the network administrator wants to introduce IPv6 into an existing IPv4 IS-IS network. To ensure that the checking of hello packet checks from adjacent neighbors is disabled until all the neighbor routers are configured to use IPv6, the network administrator enters the **no adjacency-check** command.

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# no adjacency-check
```

In IPv4, the following example shows that the network administrator wants to introduce IPv6 into an existing IPv4 IS-IS network. To ensure that the checking of hello packet checks from adjacent neighbors is disabled until all the neighbor routers are configured to use IPv6, the network administrator enters the **no adjacency-check** command.

```
Router(config)# router isis
Router(config-router-af)# no adjacency-check
```

area authentication (IPv6)

To enable authentication for an Open Shortest Path First (OSPF) area, use the **area authentication** command in router configuration mode. To remove an authentication specification of an area or a specified area from the configuration, use the **no** form of this command.

area *area-id* **authentication ipsec spi md5** [*key-encryption-type*] *key*

no area *area-id* **authentication ipsec spi spi**

| | | |
|---------------------------|----------------------------|---|
| Syntax Description | <i>area-id</i> | Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IPv6 prefix. |
| | ipsec | IP Security (IPSec). |
| | spi <i>spi</i> | Security policy index (SPI) value. The <i>spi</i> value must be a number from 256 to 4294967295, which is entered as a decimal. |
| | md5 | Enables Message Digest 5 (MD5) authentication on the area specified by the <i>area-id</i> argument. |
| | <i>key-encryption-type</i> | (Optional) One of two values can be entered: <ul style="list-style-type: none"> 0—The key is not encrypted. 7—The key is encrypted. |
| | <i>key</i> | Number used in the calculation of the message digest. The number is 32 hex digits (16 bytes) long. |
| | | |

Defaults Key encryption type 0: key is not encrypted.

Command Modes Router configuration

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 12.3(4)T | This command was introduced. |

Usage Guidelines The user needs to ensure that the same policy (the SPI and the key) is configured on all of the interfaces on the link. SPI values may automatically be used by other client applications, such as tunnels.

The policy database is common to all client applications on a box. This means that two IPSec clients, such as OSPF and a tunnel, cannot use the same SPI. Additionally, an SPI can only be used in one policy.

Examples The following example enables authentication for the OSPF area 1:

```
area 1 authentication ipsec spi 678 md5 1234567890ABCDEF1234567890ABCDEF
```

area range

To consolidate and summarize routes at an area boundary, use the **area range** command in router configuration mode. To disable this function, use the **no** form of this command.

```
area area-id range {ipv6-prefix /prefix-length} [advertise | not-advertise] [cost cost]
```

```
no area area-id range {ipv6-prefix /prefix-length} [advertise | not-advertise] [cost cost]
```

| Syntax Description | | |
|-------------------------|--|---|
| <i>area-id</i> | | Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IPv6 prefix. |
| <i>ipv6-prefix</i> | | IPv6 prefix. |
| <i>prefix-length</i> | | IPv6 prefix length. |
| 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>cost</i> | | (Optional) Metric or cost for this summary route, which is used during OSPF SPF calculation to determine the shortest paths to the destination. The value can be 0 to 16777215. |

| | |
|-----------------|--------------------------------------|
| Defaults | This command is disabled by default. |
|-----------------|--------------------------------------|

| | |
|----------------------|----------------------|
| Command Modes | Router configuration |
|----------------------|----------------------|

| Command History | Release | Modification |
|-----------------|-----------|--|
| | 10.0 | This command was introduced. |
| | 12.0(24)S | Support for IPv6 was added. The cost keyword and <i>cost</i> argument were added. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

| | |
|-------------------------|--|
| Usage Guidelines | <p>The area range command is used 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 behavior is called <i>route summarization</i>.</p> |
|-------------------------|--|

Multiple **area** router configuration commands specifying the **range** option can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

This command has been modified for OSPF for IPv6. Users can now enter the IPv6 address syntax.

**Note**

To remove the specified area from the software configuration, use the **no area *area-id*** command (with no other keywords). That is, the **no area *area-id*** command removes all area options, such as **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 10.0.0.0 and for all hosts on network 192.168.110.0:

```
interface Ethernet0/0
  no ip address
  ipv6 enable
  ipv6 ospf 1 area 1
!
ipv6 router ospf 1
  router-id 192.168.255.5
  log-adjacency-changes
  area 1 range 2001:0DB8:0:1::/64
```

The following example shows the IPv6 address syntax:

```
Router(config-rtr)# area 1 range ?

X:X:X:X::X/<0-128>  IPv6 prefix x:x::y/z
```


area virtual-link

To define an OSPF virtual link, use the **area virtual-link** command in router configuration mode with the optional parameters. To remove a virtual link, use the **no** form of this command.

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*]
[**transmit-delay** *seconds*] [**dead-interval** *seconds*]

no **area** *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*]
[**transmit-delay** *seconds*] [**dead-interval** *seconds*]

no **area** *area-id*

Syntax Description

| | |
|---|--|
| <i>area-id</i> | Area ID assigned to the transit area for the virtual link. This can be either a decimal value or a valid IPv6 prefix. There is no default. |
| <i>router-id</i> | Router ID associated with the virtual link neighbor. The router ID appears in the show ip ospf display. There is no default. |
| hello-interval <i>seconds</i> | (Optional) Time (in seconds) between the hello packets that the Cisco IOS software sends on an interface. Unsigned integer value to be advertised in the hello packets. The value must be the same for all routers and access servers attached to a common network. The default is 10 seconds. |
| retransmit-interval <i>seconds</i> | (Optional) Time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. Expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. The default is 5 seconds. |
| transmit-delay <i>seconds</i> | (Optional) Estimated time (in seconds) required to send a link-state update packet on the interface. Integer value that must be greater than zero. LSAs in the update packet have their age incremented by this amount before transmission. The default value is 1 second. |
| dead-interval <i>seconds</i> | (Optional) Time (in seconds) that hello packets are not seen before a neighbor declares the router down. Unsigned integer value. The default is four times the hello interval, or 40 seconds. As with the hello interval, this value must be the same for all routers and access servers attached to a common network. |

Defaults

area-id: No area ID is predefined.
router-id: No router ID is predefined.
hello-interval *seconds*: 10 seconds
retransmit-interval *seconds*: 5 seconds
transmit-delay *seconds*: 1 second
dead-interval *seconds*: 40 seconds

Command Modes

Router configuration

Command History

| Release | Modification |
|-----------|---|
| 10.0 | This command was introduced. |
| 12.0(24)S | Support for IPv6 was added. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines

In OSPF, 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.

The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue.

The setting of the retransmit interval should be conservative, or needless retransmissions will result. The value should be larger for serial lines and virtual links.

The transmit delay value should take into account the transmission and propagation delays for the interface.

To configure a virtual link in OSPF for IPv6, you must use a router ID instead of an address. In OSPF for IPv6, the virtual link takes the router ID rather than the IPv6 prefix of the remote router.

**Note**

For a virtual link to be properly configured, each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor router ID. To see the router ID, use the **show ip ospf** command in EXEC mode.

**Note**

To remove the specified area from the software configuration, use the **no area area-id** command (with no other keywords). That is, the **no area area-id** command removes all area options, such as **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Examples

The following example establishes a virtual link with default values for all optional parameters:

```
ipv6 router ospf 1
 log-adjacency-changes
 area 1 virtual-link 192.168.255.1
```

The following example establishes a virtual link in OSPF for IPv6:

```
ipv6 router ospf 1
 log-adjacency-changes
 area 1 virtual-link 192.168.255.1 hello-interval 5
```

atm route-bridge

To configure an interface to use the ATM routed bridge encapsulation (RBE), use the **atm route-bridge** command in interface configuration mode.

atm route-bridge *protocol*

| | | |
|---------------------------|-----------------|---|
| Syntax Description | <i>protocol</i> | Protocol to be route-bridged. IP and IPv6 are the only protocols that can be route-bridged using ATM RBE. |
|---------------------------|-----------------|---|

| | |
|-----------------|--|
| Defaults | ATM routed bridge encapsulation is not configured. |
|-----------------|--|

| | |
|----------------------|-------------------------|
| Command Modes | Interface configuration |
|----------------------|-------------------------|

| | | |
|------------------------|----------------|--|
| Command History | Release | Modification |
| | 12.0(5)DC | This command was introduced. |
| | 12.1(2)T | This command was integrated in Cisco IOS Release 12.1(2)T. |
| | 12.3(4)T | The ipv6 keyword was added to support RBE of IPv6 packets as specified in RFC 1483. |

| | |
|-------------------------|---|
| Usage Guidelines | Routing of IPv6 Packets |
| | IPv6 packets can be routed using RBE only over ATM point-to-point subinterfaces. Routing of IP packets and IPv6 half-bridging, bridging, PPP over Ethernet (PPPoE), or other Ethernet 802.3-encapsulated protocols can be configured on the same subinterface. |

Router Advertisements with IPv6

Router advertisements are suppressed by default. For stateless autoconfiguration, router advertisements must be allowed with the **no ipv6 nd suppress-ra** command. For static configuration, router advertisement is not required, however, the aggregator should either have the RBE interface on the same subnet as the client or have a static IPv6 route to that subnet through the RBE interface.

| | |
|-----------------|---------------------------------|
| Examples | IP Encapsulation Example |
|-----------------|---------------------------------|

The following example configures ATM routed bridge encapsulation on an interface:

```
interface atm 4/0.100 point-to-point
 ip address 172.16.5.9 255.255.255.0
 pvc 0/32
 atm route-bridge ip
```

IPv6 Encapsulation Example

The following example shows a typical configuration on an RBE interface to allow routing of IPv6 encapsulated Ethernet packets. IPv6 packets sent out of the subinterface are encapsulated over Ethernet over the RBE interface.

```
interface ATM1/0.1 point-to-point
  ipv6 enable
  ipv6 address 3FEE:12E1:2AC1:EA32::/64
  no ipv6 nd suppress-ra
  atm route-bridge ipv6
pvc 1/101
```

In this example, the **ipv6 enable** command allows the routing of IPv6 packets. The **ipv6 address** command specifies an IPv6 address for the interface and an IPv6 prefix to be advertised to a peer. The **no ipv6 nd suppress-ra** command enables router advertisements on the interface.

IPv6 Routing and Bridging of Other Traffic Example

The following example shows a configuration in which IPv6 packets are routed and all other packets are bridged.

```
interface ATM1/0.1 point-to-point
  ipv6 enable
  ipv6 address 3FEE:12E1:2AC1:EA32::/64
  atm route-bridge ipv6
  bridge-group 1
pvc 1/101
```

IP and IPv6 Routing with Bridging of Other Protocols Example

IP and IPv6 routing can be configured on the same interface as shown in this example. All other packets are bridged. PPPoE could also be configured on this same interface.

```
interface ATM1/0.1 point-to-point
  ipv6 enable
  ipv6 address 3FEE:12E1:2AC1:EA32::/64
  ip address 10.0.0.1 255.255.255.0
  atm route-bridge ipv6
  atm route-bridge ip
  bridge-group 1
pvc 1/101
```

Static Configuration Example

The following example shows the IPv6 static route configured. Unlike, IP, the IPv6 interface on an aggregator is always numbered and, minimally, has a link local IPv6 address.

```
router# configure terminal
router(config)# ipv6 route 3FEE:12E1:2AC1:EA32::/64 atm1/0.3
router(config)# end
router#
```

show ipv6 interface Example

Notice in this **show ipv6 interface** output display that each RBE link has its own subnet prefix. Unlike proxy ARP in IPv4 RBE configurations, the aggregator does not require proxy ND in IPv6 RBE deployments.

```
router#show ipv6 interface atm1/0.1

ATM1/0.1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFE:FE3B:B400
```

```
Global unicast address(es):
  3FEE:12E1:2AC1:EA32::, subnet is 3FEE:12E1:2AC1:EA32::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:0
  FF02::1:FF3B:B400
MTU is 4470 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses
```

Related Commands

| Command | Description |
|-------------------------------|--|
| no ipv6 nd suppress-ra | Suppresses IPv6 router advertisement transmissions on a LAN interface. |

clear bgp ipv6

To reset IPv6 Border Gateway Protocol (BGP) sessions, use the **clear bgp ipv6** command in privileged EXEC mode.

clear bgp ipv6 { **unicast** | **multicast** } { * | *autonomous-system-number* | *ip-address* | *ipv6-address* | *peer-group-name* } [**soft**] [**in** | **out**]

Syntax Description

| | |
|---------------------------------|---|
| unicast | Specifies IPv6 unicast address prefixes. |
| multicast | Specifies IPv6 multicast address prefixes. |
| * | Resets all current BGP sessions. |
| <i>autonomous-system-number</i> | Resets BGP sessions for BGP neighbors within the specified autonomous system. |
| <i>ip-address</i> | Resets the TCP connection to the specified IPv4 BGP neighbor and removes all routes learned from the connection from the BGP table. |
| <i>ipv6-address</i> | Resets the TCP connection to the specified IPv6 BGP neighbor and removes all routes learned from the connection from the BGP table. 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>peer-group-name</i> | Resets the TCP connection to the specified IPv6 BGP neighbor and removes all routes learned from the connection from the BGP table. |
| soft | (Optional) Soft reset. Does not reset the session. |
| in out | (Optional) Triggers inbound or outbound soft reconfiguration. If the in or out option is not specified, both inbound and outbound soft resets are triggered. |

Defaults

No reset is initiated.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------|---|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.3(2)T | The unicast keyword was added. |
| 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines

The **clear bgp ipv6** command is similar to the **clear ip bgp** command, except that it is IPv6-specific.

Use of the **clear bgp ipv6** command allows a reset of the neighbor sessions with varying degrees of severity depending on the specified keywords and arguments.

Use the **clear bgp ipv6 unicast** command to drop neighbor sessions with IPv6 unicast address prefixes.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Use the **clear bgp ipv6 *** command to drop all neighbor sessions. The Cisco IOS software will then reset the neighbor connections. Use this form of the command in the following situations:

- BGP timer specification change
- BGP administrative distance changes

Use the **clear bgp ipv6 soft out** or the **clear bgp ipv6 unicast soft out** command to drop only the outbound neighbor connections. Inbound neighbor sessions will not be reset. Use this form of the command in the following situations:

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

Use the **clear bgp ipv6 soft in** or the **clear bgp ipv6 unicast soft in** command to drop only the inbound neighbor connections. Outbound neighbor sessions will not be reset. To reset inbound routing table updates dynamically for a neighbor, you must configure the neighbor to support the router refresh capability. To determine whether a BGP neighbor supports this capability, use the **show bgp ipv6 neighbors** or the **show bgp ipv6 unicast neighbors** command. If a neighbor supports the route refresh capability, the following message is displayed:

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

If all BGP networking devices support the route refresh capability, use the **clear bgp ipv6 { * | ip-address | ipv6-address | peer-group-name } in** or the **clear bgp ipv6 unicast { * | ip-address | ipv6-address | peer-group-name } in** command. Use of the **soft** keyword is not required when the route refresh capability is supported by all BGP networking devices, because the software automatically performs a soft reset.

Use this form of the command in the following situations:

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

Examples

The following example clears the inbound session with the neighbor 7000::2 without the outbound session being reset:

```
Router# clear bgp ipv6 7000::2 soft in
```

clear bgp ipv6

The following example uses the **unicast** keyword and clears the inbound session with the neighbor 7000::2 without the outbound session being reset:

```
Router# clear bgp ipv6 unicast 7000::2 soft in
```

The following example clears the outbound session with the peer group named marketing without the inbound session being reset:

```
Router# clear bgp ipv6 marketing soft out
```

The following example uses the **unicast** keyword and clears the outbound session with the peer group named peer-group marketing without the inbound session being reset:

```
Router# clear bgp ipv6 unicast peer-group marketing soft out
```

Related Commands

| Command | Description |
|----------------------|---|
| show bgp ipv6 | Displays entries in the IPv6 BGP routing table. |

clear bgp ipv6 dampening

To clear IPv6 Border Gateway Protocol (BGP) route dampening information and unsuppress the suppressed routes, use the **clear bgp ipv6 dampening** command in privileged EXEC mode.

```
clear bgp ipv6 {unicast | multicast} dampening [ipv6-prefix/prefix-length]
```

| | | |
|--------------------|-----------------------|---|
| Syntax Description | unicast | Specifies IPv6 unicast address prefixes. |
| | multicast | Specifies IPv6 multicast address prefixes. |
| | <i>ipv6-prefix</i> | (Optional) IPv6 network about which to clear dampening information. 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> | (Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |

Defaults

When the *ipv6-prefix/prefix-length* argument is not specified, the **clear bgp ipv6 dampening** command clears route dampening information for the entire IPv6 BGP routing table.

As of Cisco IOS Release 12.3(2)T, when the *ipv6-prefix/prefix-length* argument is not specified, the **clear bgp ipv6 unicast dampening** command clears route dampening information for the entire IPv6 BGP routing table.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------|---|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.3(2)T | The unicast keyword was added. |
| 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines

The **clear bgp ipv6 dampening** and the **clear bgp ipv6 unicast dampening** commands are similar to the **clear ip bgp dampening** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following example clears route dampening information about the route to network 7000::0 and unsuppresses its suppressed routes:

```
Router# clear bgp ipv6 dampening 7000::/64
```

The following example uses the **unicast** keyword and clears route dampening information about the route to network 7000::0 and unsuppresses its suppressed routes:

```
Router# clear bgp ipv6 unicast dampening 7000::/64
```

Related Commands

| Command | Description |
|-------------------------------------|---|
| bgp dampening | Enables BGP route dampening or changes various BGP route dampening factors. |
| show bgp ipv6 dampened-paths | Displays IPv6 BGP dampened routes. |

clear bgp ipv6 external

To clear external IPv6 Border Gateway Protocol (BGP) peers, use the **clear bgp ipv6 external** command in privileged EXEC mode.

clear bgp ipv6 {unicast | multicast} external [soft] [in | out]

| | | |
|--------------------|------------------|--|
| Syntax Description | unicast | Specifies IPv6 unicast address prefixes. |
| | multicast | Specifies IPv6 multicast address prefixes. |
| | soft | (Optional) Soft reset. Does not reset the session. |
| | in out | (Optional) Triggers inbound or outbound soft reconfiguration. If the in or out option is not specified, both inbound and outbound soft resets are triggered. |

| | |
|---------------|-----------------|
| Command Modes | Privileged EXEC |
|---------------|-----------------|

| | | |
|-----------------|----------------|---|
| Command History | Release | Modification |
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| | 12.3(2)T | The unicast keyword was added. |
| | 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines The **clear bgp ipv6 external** command is similar to the **clear ip bgp external** command, except that it is IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples The following example clears the inbound session with external IPv6 BGP peers without the outbound session being reset:

```
Router# clear bgp ipv6 external soft in
```

The following example uses the **unicast** keyword and clears the inbound session with external IPv6 BGP peers without the outbound session being reset:

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

 clear bgp ipv6 external**Related Commands**

| Command | Description |
|----------------|--|
| clear bgp ipv6 | Resets an IPv6 BGP connection by dropping all neighbor sessions. |

clear bgp ipv6 flap-statistics

To clear IPv6 Border Gateway Protocol (BGP) flap statistics, use the **clear bgp ipv6 flap-statistics** command in privileged EXEC mode.

```
clear bgp ipv6 {unicast | multicast} flap-statistics [ipv6-prefix/prefix-length | regexp regexp |
filter-list list]
```

Syntax Description

| | |
|--------------------------------|---|
| unicast | Specifies IPv6 unicast address prefixes. |
| multicast | Specifies IPv6 multicast address prefixes. |
| <i>ipv6-prefix</i> | (Optional) Clears flap statistics for a single entry at this IPv6 network. 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> | (Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |
| regexp <i>regexp</i> | (Optional) Clears flap statistics for all the paths that match the regular expression. |
| filter-list <i>list</i> | (Optional) Clears flap statistics for all the paths that pass the access list. The acceptable access list number range is from 1 to 199. |

Defaults

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

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------|---|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.3(2)T | The unicast keyword was added. |
| 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines

The **clear bgp ipv6 flap-statistics** command is similar to the **clear ip bgp flap-statistics** command, except that it is IPv6-specific.

The flap statistics for a route are also cleared when an IPv6 BGP peer is reset. Although the reset withdraws the route, no penalty is applied in this instance even though route flap dampening is enabled.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following example clears all of the flap statistics for paths that pass access list 3:

```
Router# clear bgp ipv6 flap-statistics filter-list 3
```

The following example uses the **unicast** keyword and clears all of the flap statistics for paths that pass access list 3:

```
Router# clear bgp ipv6 unicast flap-statistics filter-list 3
```

Related Commands

| Command | Description |
|--------------------------------------|---|
| bgp dampening | Enables BGP route dampening or changes various BGP route dampening factors. |
| show bgp ipv6 flap-statistics | Displays IPv6 BGP flap statistics. |

clear bgp ipv6 peer-group

To clear all members of an IPv6 Border Gateway Protocol (BGP) peer group, use the **clear bgp ipv6 peer-group** command in privileged EXEC mode.

```
clear bgp ipv6 {unicast | multicast} peer-group [name]
```

Syntax Description

| | |
|------------------|--|
| unicast | Specifies IPv6 unicast address prefixes. |
| multicast | Specifies IPv6 multicast address prefixes. |
| <i>name</i> | BGP peer group name. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.3(2)T | This command was introduced. |
| 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines

Using the **clear bgp ipv6 peer-group** command without the optional *name* argument will clear all BGP peer groups.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following example clears all IPv6 BGP peer groups:

```
Router# clear bgp ipv6 unicast peer-group
```

clear ipv6 access-list

To reset the IPv6 access list match counters, use the **clear ipv6 access-list** command in privileged EXEC mode.

clear ipv6 access-list [*access-list-name*]

Syntax Description

| | |
|-------------------------|---|
| <i>access-list-name</i> | (Optional) Name of the IPv6 access list for which to clear the match counters. Names cannot contain a space or quotation mark, or begin with a numeric. |
|-------------------------|---|

Defaults

No reset is initiated.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.0(23)S | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **clear ipv6 access-list** command is similar to the **clear ip access-list counters** command, except that it is IPv6-specific.

The **clear ipv6 access-list** command used without the *access-list-name* argument resets the match counters for all IPv6 access lists configured on the router.

Examples

The following example resets the match counters for the IPv6 access list named marketing:

```
Router# clear ipv6 access-list marketing
```

Related Commands

| Command | Description |
|------------------------------|---|
| ipv6 access-list | Defines an IPv6 access list and enters IPv6 access list configuration mode. |
| show ipv6 access-list | Displays the contents of all current IPv6 access lists. |

clear ipv6 dhcp binding

To delete automatic client bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 binding table, use the **clear ipv6 dhcp binding** command in privileged EXEC mode.

clear ipv6 dhcp binding [*ipv6-address*]

| | | |
|--------------------|---------------------|--|
| Syntax Description | <i>ipv6-address</i> | (Optional) The address of a DHCP for IPv6 client. |
| | | This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |

| | |
|---------------|-----------------|
| Command Modes | Privileged EXEC |
|---------------|-----------------|

| | | |
|-----------------|----------|------------------------------|
| Command History | Release | Modification |
| | 12.3(4)T | This command was introduced. |

| | |
|------------------|---|
| Usage Guidelines | The clear ipv6 dhcp binding command is used as a server function. |
| | <p>A binding table entry on the DHCP for IPv6 server is automatically:</p> <ul style="list-style-type: none">• Created whenever a prefix is delegated to a client from the configuration pool• Updated when the client renews, rebinds, or confirms the prefix delegation• Deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or an administrator runs the clear ipv6 dhcp binding command. <p>If the clear ipv6 dhcp binding command is used with the optional <i>ipv6-address</i> argument specified, only the binding for the specified client is deleted. If the clear ipv6 dhcp binding command is used without the <i>ipv6-address</i> argument, then all automatic client bindings are deleted from the DHCP for IPv6 binding table.</p> |

| | |
|----------|--|
| Examples | The following example deletes all automatic client bindings from the DHCP for IPv6 server binding table: |
| | <pre>Router# clear ipv6 dhcp binding</pre> |

| | | |
|------------------|-------------------------------|---|
| Related Commands | Command | Description |
| | show ipv6 dhcp binding | Displays automatic client bindings from the DHCP for IPv6 server binding table. |

clear ipv6 dhcp client

To restart the Dynamic Host Configuration Protocol (DHCP) for IPv6 client on an interface, use the **clear ipv6 dhcp client** command in privileged EXEC mode.

clear ipv6 dhcp client *interface-type interface-number*

Syntax Description

| | |
|-------------------------|--|
| <i>interface-type</i> | Interface type and number. For more information, use the question mark (?) online help function. |
| <i>interface-number</i> | |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|----------|------------------------------|
| 12.3(4)T | This command was introduced. |

Usage Guidelines

The **clear ipv6 dhcp client** command restarts the DHCP for IPv6 client on specified interface after first releasing and unconfiguring previously acquired prefixes and other configuration options (for example, Domain Name System [DNS] servers).

Examples

The following example restarts the DHCP for IPv6 client for Ethernet interface 1/0:

```
Router# clear ipv6 dhcp client Ethernet 1/0
```

Related Commands

| Command | Description |
|---------------------------------|---|
| show ipv6 dhcp interface | Displays DHCP for IPv6 interface information. |

clear ipv6 mfib counters

To reset all active Multicast Forwarding Information Base (MFIB) traffic counters, use the **clear ipv6 mfib counters** command in privileged EXEC mode.

clear ipv6 mfib counters [*group-name* | *group-address* [*source-address* | *source-name*]]

Syntax Description

| | |
|---|---|
| <i>group-name</i> <i>group-address</i> | (Optional) IPv6 address or name of the multicast group. |
| <i>source-address</i> <i>source-name</i> | (Optional) IPv6 address or name of the source. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.3(2)T | This command was introduced. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

After you enable the **clear ipv6 mfib counters** command, you can determine if additional traffic is forwarded by using one of the following show commands that display traffic counters:

- **show ipv6 mfib**
- **show ipv6 mfib active**
- **show ipv6 mfib count**
- **show ipv6 mfib interface**
- **show ipv6 mfib summary**

Examples

The following example clears and resets all MFIB traffic counters:

```
Router# clear ipv6 mfib counters
```

clear ipv6 mld counters

To clear the Multicast Listener Discovery (MLD) interface counters, use the **clear ipv6 mld counters** command in privileged EXEC mode.

clear ipv6 mld counters [*interface-type*]

Syntax Description

| | |
|-----------------------|--|
| <i>interface-type</i> | (Optional) Interface type. For more information, use the question mark (?) online help function. |
|-----------------------|--|

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|--|
| 12.0(26)S | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines

Use the **clear ipv6 mld counters** command to clear the MLD counters, which keep track of the number of joins and leaves received. If you omit the optional interface-type argument, the **clear ipv6 mld counters** command clears the counters on all interfaces.

Examples

The following example clears the counters for Ethernet interface 1/0:

```
clear ipv6 mld counters Ethernet1/0
```

Related Commands

| Command | Description |
|--------------------------------|--|
| show ipv6 mld interface | Displays multicast-related information about an interface. |

clear ipv6 mld traffic

To reset the Multicast Listener Discovery (MLD) traffic counters, use the **clear ipv6 mld traffic** command in privileged EXEC mode.

clear ipv6 mld traffic

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|--|
| | 12.0(26)S | This command was introduced. |
| | 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines Using the **clear ipv6 mld traffic** command will reset all MLD traffic counters.

Examples The following example resets the MLD traffic counters:

```
clear ipv6 mld traffic
```

| Related Commands | Command | Description |
|------------------|-----------------------|------------------------------------|
| | show ipv6 mld traffic | Displays the MLD traffic counters. |

clear ipv6 nat translation

To clear dynamic Network Address Translation - Protocol Translation (NAT-PT) translations from the dynamic state table, use the **clear ipv6 nat translation** command in EXEC mode.

clear ipv6 nat translation *

| | |
|---------------------------|--|
| Syntax Description | * Clears all dynamic NAT-PT translations. |
|---------------------------|--|

| | |
|-----------------|--|
| Defaults | Entries are deleted from the dynamic translation state table when they time out. |
|-----------------|--|

| | |
|----------------------|------|
| Command Modes | EXEC |
|----------------------|------|

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 12.2(13)T | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | Use this command to clear entries from the dynamic translation state table before they time out. Static translation configuration is not affected by this command. |
|-------------------------|--|

| | |
|-----------------|---|
| Examples | The following example shows the NAT-PT entries before and after the dynamic translation state table is cleared. Note that all the dynamic NAT-PT mappings are cleared, but the static NAT-PT configurations remain. |
|-----------------|---|

Router# **show ipv6 nat translations**

```

Prot  IPv4 source      IPv6 source
     IPv4 destination  IPv6 destination
---  ---
     192.168.123.2    2001::2

---  ---
     192.168.122.10   2001::10

tcp   192.168.124.8,11047  3002::8,11047
     192.168.123.2,23  2001::2,23

udp   192.168.124.8,52922  3002::8,52922
     192.168.123.2,69  2001::2,69

```

Router# **clear ipv6 nat translation**

```
Router# show ipv6 nat translations

Prot  IPv4 source      IPv6 source
      IPv4 destination  IPv6 destination
---  ---
      192.168.123.2      2001::2
---  ---
      192.168.122.10     2001::10
```

| Related Commands | Command | Description |
|------------------|----------------------------|--|
| | ipv6 nat | Designates that traffic originating from or destined for the interface is subject to NAT-PT. |
| | show ipv6 nat translations | Displays active NAT-PT translations. |

clear ipv6 neighbors

To delete all entries in the IPv6 neighbor discovery cache, except static entries, use the **clear ipv6 neighbors** command in privileged EXEC mode.

clear ipv6 neighbors

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release | Modification |
|------------------------|------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

| | |
|-----------------|---|
| Examples | The following example deletes all entries, except static entries, in the neighbor discovery cache: Router# clear ipv6 neighbors |
|-----------------|---|

| Related Commands | Command | Description |
|-------------------------|----------------------------|---|
| | ipv6 neighbor | Configures a static entry in the IPv6 neighbor discovery cache. |
| | show ipv6 neighbors | Displays IPv6 neighbor discovery cache information. |

clear ipv6 ospf

To clear the OSPF state based on the OSPF routing process ID, use the **clear ipv6 ospf** command in privileged EXEC mode.

```
clear ipv6 ospf [process-id] {process | force-spf | redistribution | counters [neighbor [neighbor-interface]]}
```

| Syntax Description | <i>process-id</i> | (Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process. |
|--------------------|---------------------------|--|
| | process | Restarts the OSPF process. |
| | force-spf | Starts the shortest path first (SPF) algorithm without first clearing the OSPF database. |
| | redistribution | Clears OSPF route redistribution. |
| | counters | Resets OSPF counters. |
| | neighbor | (Optional) Neighbor counters per interface. |
| | <i>neighbor-interface</i> | (Optional) Neighbor interface. |

| Command Modes | Privileged EXEC |
|---------------|-----------------|
|---------------|-----------------|

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines

When the **process** keyword is used with the **clear ipv6 ospf** command, the OSPF database is cleared and repopulated, and then the shortest path first (SPF) algorithm is performed. When the **force-spf** keyword is used with the **clear ipv6 ospf** command, the OSPF database is not cleared before the SPF algorithm is performed.

Use the *process-id* option to clear only one OSPF process. If the *process-id* option is not specified, all OSPF processes are cleared.

Examples

The following example starts the SPF algorithm without clearing the OSPF database:

```
Router# clear ipv6 ospf force-spf
```

clear ipv6 pim counters

To reset the Protocol Independent Multicast (PIM) traffic counters, use the **clear ipv6 pim counters** command in privileged EXEC mode.

clear ipv6 pim counters

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|--|
| | 12.0(26)S | This command was introduced. |
| | 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines Using the **clear ipv6 pim counters** command will reset all PIM traffic counters.

Examples The following example resets the PIM traffic counters:

```
clear ipv6 pim counters
```

| Related Commands | Command | Description |
|------------------|-----------------------|------------------------------------|
| | show ipv6 pim traffic | Displays the PIM traffic counters. |

clear ipv6 pim reset

To delete all entries from the topology table and reset the Multicast Routing Information Base (MRIB) connection, use the **clear ipv6 pim reset** command in privileged EXEC mode.

clear ipv6 pim reset

Syntax Description

The command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.3(2)T | This command was introduced. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

Using the **clear ipv6 pim reset** command breaks the PIM-MRIB connection, clears the topology table, and then reestablishes the PIM-MRIB connection. This procedure forces MRIB resynchronization.



Caution

Use the **clear ipv6 pim reset** command with caution, as it clears all PIM protocol information from the PIM topology table. Use of the **clear ipv6 pim reset** command should be reserved for situations where PIM and MRIB communication are malfunctioning.

Examples

The following example deletes all entries from the topology table and resets the MRIB connection:

```
Router# clear ipv6 pim reset
```

clear ipv6 pim topology

To clear the Protocol Independent Multicast (PIM) topology table, use the **clear ipv6 pim topology** command in privileged EXEC mode.

```
clear ipv6 pim topology [group-name | group-address]
```

| | | |
|--------------------|--|---|
| Syntax Description | <i>group-name</i> <i>group-address</i> | (Optional) IPv6 address or name of the multicast group. |
|--------------------|--|---|

| | |
|----------|--|
| Defaults | When the command is used with no arguments, all group entries located in the PIM topology table are cleared of PIM protocol information. |
|----------|--|

| | |
|---------------|-----------------|
| Command Modes | Privileged EXEC |
|---------------|-----------------|

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

| | |
|------------------|---|
| Usage Guidelines | This command clears PIM protocol information from all group entries located in the PIM topology table. Information obtained from the MRIB table is retained. If a multicast group is specified, only those group entries are cleared. |
|------------------|---|

| | |
|----------|---|
| Examples | <p>The following example clears all group entries located in the PIM topology table:</p> <pre>Router# clear ipv6 pim topology</pre> |
|----------|---|

clear ipv6 prefix-list

To reset the hit count of the IPv6 prefix list entries, use the **clear ipv6 prefix-list** command in privileged EXEC mode.

clear ipv6 prefix-list [*prefix-list-name*] [*ipv6-prefix/prefix-length*]

| | | |
|--------------------|-------------------------|---|
| Syntax Description | <i>prefix-list-name</i> | (Optional) The name of the prefix list from which the hit count is to be cleared. |
| | <i>ipv6-prefix</i> | (Optional) The IPv6 network from which the hit count is to be cleared. 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> | (Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |

Defaults Clears the hit count for all IPv6 prefix lists.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |


Usage Guidelines The **clear ipv6 prefix-list** command is similar to the **clear ip prefix-list** command, except that it is IPv6-specific.

The hit count is a value indicating the number of matches to a specific prefix list entry.

Examples The following example clears the hit count from the prefix list entries for the prefix list named first_list that match the network mask 2001:0DB8::/35.

```
Router# clear ipv6 prefix-list first_list 2001:0DB8::/35
```

| Related Commands | Command | Description |
|------------------|------------------|--|
| | ipv6 prefix-list | Creates an entry in an IPv6 prefix list. |

 **clear ipv6 prefix-list**

| | |
|---|--|
| ipv6 prefix-list sequence-number | Enables the generation of sequence numbers for entries in an IPv6 prefix list. |
| show ipv6 prefix-list | Displays information about an IPv6 prefix list or prefix list entries. |

clear ipv6 rip

To delete routes from the IPv6 Routing Information Protocol (RIP) routing table, use the **clear ipv6 rip** command in privileged EXEC mode.

clear ipv6 rip [*name*]

Syntax Description

| | |
|------|---|
| name | (Optional) Name of an IPv6 RIP process. |
|------|---|

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.0(22)S | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

When the *name* argument is specified, only routes for that process are deleted from the IPv6 RIP routing table and, if installed, from the IPv6 routing table. If no *name* argument is specified, all IPv6 RIP routes are deleted.

Use the **show ipv6 rip** command to display IPv6 RIP routes.

Examples

The following example deletes all the IPv6 routes for the RIP process called one;

```
Router# clear ipv6 rip one
```

Related Commands

| Command | Description |
|----------------------|--|
| show ipv6 rip | Displays the current contents of the IPv6 RIP routing table. |

clear ipv6 route

To delete routes from the IPv6 routing table, use the **clear ipv6 route** command in privileged EXEC mode.

```
clear ipv6 route {ipv6-address | ipv6-prefix/prefix-length | *}
```

Syntax Description

| | |
|----------------|--|
| ipv6-address | The address of the IPv6 network to delete from the table. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| ipv6-prefix | The IPv6 network number to delete from the table. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| /prefix-length | The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |
| * | Clears all IPv6 routes. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **clear ipv6 route** command is similar to the **clear ip route** command, except that it is IPv6-specific. When the *ipv6-address* or *ipv6-prefix/length* argument is specified, only that route is deleted from the IPv6 routing table. When the *** keyword is specified, all routes are deleted from the routing table (the per-destination maximum transmission unit [MTU] cache is also cleared).

Examples

The following example deletes the IPv6 network 2001:0DB8::/35.

```
Router# clear ipv6 route 2001:0DB8::/35
```

Related Commands

| Command | Description |
|------------------------|--|
| ipv6 route | Establishes static IPv6 routes. |
| show ipv6 route | Displays the current contents of the IPv6 routing table. |

clear ipv6 traffic

To reset IPv6 traffic counters, use the **clear ipv6 traffic** command in privileged EXEC mode.

clear ipv6 traffic

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S and output fields were added. |
| | 12.2(13)T | The modification to add output fields was integrated into this release. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines Using this command resets the counters in the output from the **show ipv6 traffic** command.

Examples The following example resets the IPv6 traffic counters. The output from the **show ipv6 traffic** command shows that the counters are reset:

```
Router# clear ipv6 traffic
```

```
Router# show ipv6 traffic
```

```
IPv6 statistics:
```

```
  Rcvd:  1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  1 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent
```

```
ICMP statistics:
```

```
  Rcvd: 1 input, 0 checksum errors, 0 too short
         0 unknown info type, 0 unknown error type
  unreachable: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
  parameter: 0 error, 0 header, 0 option
         0 hopcount expired, 0 reassembly timeout, 0 too big
         0 echo request, 0 echo reply
         0 group query, 0 group report, 0 group reduce
```

```

0 router solicit, 0 router advert, 0 redirects
0 neighbor solicit, 1 neighbor advert
Sent: 1 output
  unreachable: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
  parameter: 0 error, 0 header, 0 option
  0 hopcount expired, 0 reassembly timeout, 0 too big
  0 echo request, 0 echo reply
  0 group query, 0 group report, 0 group reduce
  0 router solicit, 0 router advert, 0 redirects
  0 neighbor solicit, 1 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted

```

Related Commands

| Command | Description |
|--------------------------|-----------------------------------|
| show ipv6 traffic | Displays IPv6 traffic statistics. |

copy

To copy any file from a source to a destination, use the **copy** command in privileged EXEC mode.

copy [/erase] *source-url destination-url*

Syntax Description

| | |
|------------------------|---|
| /erase | (Optional) Erases the destination file system before copying. |
| <i>source-url</i> | The location URL or alias of the source file or directory to be copied. |
| <i>destination-url</i> | The destination URL or alias of the copied file or directory. |

The exact format of the source and destination URLs varies according to the file or directory location. You may enter either an alias keyword for a particular file or an alias keyword for a file system type (not a file within a type).



Timesaver

Aliases are used to reduce the amount of typing you need to perform. For example, it is easier to type **copy run start** (the abbreviated form of the **copy running-config startup-config** command) than it is to type **copy system:r nvram:s** (the abbreviated form of the **copy system:running-config nvram:startup-config** command). These aliases also allow you to continue using some of the common commands used in previous versions of Cisco IOS software.

Table 1 specifies two keyword shortcuts to URLs.

Table 1 Common Keyword Aliases to URLs

| Keyword | Source or Destination |
|-----------------------|---|
| running-config | <p>(Optional) Keyword alias for the system:running-config URL.</p> <p>The system:running-config keyword represents the current running configuration file.</p> <p>This keyword does not work in more and show file command syntaxes.</p> |
| startup-config | <p>(Optional) Keyword alias for the nvram:startup-config URL.</p> <p>The nvram:startup-config keyword represents the configuration file used during initialization (startup). This file is contained in NVRAM for all platforms except the Cisco 7000 series of routers, which use the CONFIG_FILE environment variable to specify the startup configuration. The Cisco 4500 series routers cannot use the copy running-config startup-config command.</p> <p>This keyword does not work in more and show file command syntaxes.</p> |

The next tables list aliases by file system type. If you do not specify an alias, the router looks for a file in the current directory.

Table 2 lists URL aliases for special (opaque) file systems. Table 3 lists them for network file systems, and Table 4 lists them for local writable storage file systems.

Table 2 URL Prefix Aliases for Special File Systems

| Alias | Source or Destination |
|----------------|--|
| flh: | Source URL for Flash load helper log files. |
| modem: | Destination URL for loading modem firmware on Cisco 5200 and 5300 series routers. |
| nvr: | NVRAM of the router. You can copy the startup configuration into or from NVRAM. You can also display the size of a private configuration file. |
| null: | Null destination for copies or files. You can copy a remote file to null to determine its size. |
| system: | Source or destination URL for system memory, which includes the running configuration. |
| xmodem: | Source destination for the file from a network machine that uses the Xmodem protocol. |
| ymodem: | Source destination for the file from a network machine that uses the Ymodem protocol. |

Table 3 URL Prefix Aliases for Network File Systems

| Alias | Source or Destination |
|--------------|---|
| ftp: | Source or destination URL for an FTP network server. The syntax for this alias is ftp:[[/username [:password]@] location]/directory]/filename. |
| rcp: | Source or destination URL for a Remote Copy Protocol (rcp) network server. The syntax for this alias is rcp:[[/username@]location]/directory]/filename. |
| tftp: | Source or destination URL for a TFTP network server. The syntax for this alias is tftp:[[/location]/directory]/filename. |

The URL prefix aliases for network file systems use the default network port numbers for the FTP, rcp, and TFTP protocols. The network port number identifies the network server for each protocol. The default port number for a protocol is used if a port number is not specified in the URL prefix alias. Another port number may be specified in the URL prefix aliases for FTP, rcp, and TFTP connections to network servers; however, we do not recommend specifying port numbers other than the default for these protocols because doing so may cause anomalies in your network.

The **copy** command supports the **ftp:**, **rcp:**, and **tftp:** the aliases for network file systems over an IPv4 transport; only the **tftp:** alias is supported over an IPv6 transport.

**Note**

In Cisco IOS Release 12.2(8)T or a later release, a literal IPv6 address specified with a port number must be enclosed in square brackets ([]) when the address is used in TFTP source or destination URLs; a literal IPv6 address specified without a port number need not be enclosed in square brackets.

Table 4 URL Prefix Aliases for Local Writable Storage File Systems

| Alias | Source or Destination |
|--------------------------|---|
| bootflash: | Source or destination URL for boot flash memory. |
| disk0: and disk1: | Source or destination URL of rotating media. |
| flash: | Source or destination URL for Flash memory. This alias is available on all platforms. For platforms that lack a Flash device, note that flash: is aliased to slot0: , allowing you to refer to the main Flash memory storage area on all platforms. |
| slavebootflash: | Source or destination URL for internal Flash memory on the slave Route Switch Processor (RSP) card of a router configured for High System Availability (HSA). |
| slaveram: | NVRAM on a slave RSP card of a router configured for HSA. |
| slaveslot0: | Source or destination URL of the first Personal Computer Memory Card International Association (PCMCIA) card on a slave RSP card of a router configured for HSA. |
| slaveslot1: | Source or destination URL of the second PCMCIA slot on a slave RSP card of a router configured for HSA. |
| slot0: | Source or destination URL of the first PCMCIA Flash memory card. |
| slot1: | Source or destination URL of the second PCMCIA Flash memory card. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------|---|
| 11.3 T | This command was introduced. |
| 12.2(2)T | Support was added for IPv6 addresses in source and destination URLs. |
| 12.2(8)T | Support for literal IPv6 addresses enclosed in square brackets ([])—as specified by RFC 2732, <i>Format for Literal IPv6 Addresses in URL's</i> —was added. Specifically, a literal IPv6 address specified with a port number must be enclosed in square brackets when the address is used in TFTP source or destination URLs; a literal IPv6 address specified without a port number need not be enclosed in square brackets. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

You can enter on the command line all necessary source- and destination-URL information and the username and password to use, or you can enter **copy** and have the router prompt you for any missing information.

If you enter information, choose one of the following three options: the **running-config** command, the **startup-config** command, or a file system alias (see tables.) The location of a file system dictates the format of the source or destination URL.

The colon is required after the alias. However, earlier commands not requiring a colon will remain supported, but unavailable in context-sensitive help.

The entire copying process may take several minutes. The time differs from protocol to protocol and from network to network.

In the alias syntax for **ftp:**, **rcp:**, and **tftp:** the location is either an IP address or a host name. The system also recognizes IPv6 addresses used with the **tftp:** alias syntax. (The **copy** command supports the **ftp:**, **rcp:**, and **tftp:** the aliases for network file systems over an IPv4 transport; only the **tftp:** alias is supported over an IPv6 transport.) The filename is specified relative to the directory used for file transfers.

This section contains usage guidelines for the following topics:

- Understanding Invalid Combinations of Source and Destination
- Understanding Character Descriptions
- Understanding Partitions
- Using rcp
- Using FTP
- Storing Images on Servers
- Copying from a Server to Flash Memory
- Verifying Images
- Copying a Configuration File from a Server to the Running Configuration
- Copying a Configuration File from a Server to the Startup Configuration
- Storing the Running or Startup Configuration on a Server
- Saving the Running Configuration to the Startup Configuration
- Using CONFIG_FILE, BOOTLDR, and BOOT Environment Variables
- Using the copy Command with HSA

Understanding Invalid Combinations of Source and Destination

Some invalid combinations of source and destination exist. Specifically, you cannot copy in the following directions:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the **copy flash: flash:** command is invalid)

Understanding Character Descriptions

Table 5 describes the characters that you may see during processing of the **copy** command.

Table 5 *copy Character Descriptions*

| Character | Description |
|-----------|--|
| ! | For network transfers, an exclamation point indicates that the copy process is taking place. Each exclamation point indicates the successful transfer of ten packets (512 bytes each). |
| . | For network transfers, a period indicates that the copy process timed out. Many periods in a row typically means that the copy process may fail. |
| O | For network transfers, an uppercase O indicates that a packet was received out of order and the copy process may fail. |
| e | For Flash erasures, a lowercase e indicates that a device is being erased. |
| E | An uppercase E indicates an error. The copy process may fail. |
| V | A series of uppercase Vs indicates the progress during the verification of the image checksum. |

Understanding Partitions

You cannot copy an image or configuration file to a Flash partition from which you are currently running. For example, if partition 1 is running the current system image, copy the configuration file or image to partition 2. Otherwise, the copy operation will fail.

You can identify the available Flash partitions by entering the **show file system EXEC** command.

Using rcp

The rcp protocol requires a client to send a remote username upon each rcp request to a server. When you copy a configuration file or image between the router and a server using rcp, the Cisco IOS software sends the first valid username it encounters in the following list:

1. The remote username specified in the **copy** command, if a username is specified.
2. The username set by the **ip rcmd remote-username** global configuration command, if the command is configured.
3. The remote username associated with the current tty (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the router software sends the Telnet username as the remote username.
4. The router host name.

For the rcp copy request to process successfully, an account must be defined on the network server for the remote username. If the network administrator of the destination server did not establish an account for the remote username, this command will not run successfully. If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the remote username on the server. For example, if the system image resides in the home directory of a user on the server, specify the name of that user as the remote username.

If you are writing to the server, the rcp server must be properly configured to accept the rcp write request from the user on the router. For UNIX systems, add an entry to the `.rhosts` file for the remote user on the rcp server. Suppose the router contains the following configuration lines:

```
hostname Rtr1
ip rcmd remote-username User0
```

If the IP address of the router translates to Router1.company.com, then the `.rhosts` file for User0 on the rcp server should contain the following line:

Router1.company.com Rtr1

Refer to the documentation for your rcp server for more details.

If you are using a personal computer as a file server, the computer must support rsh (remote shell protocol).

Using FTP

The FTP protocol requires a client to send a remote username and password upon each FTP request to a server. When you copy a configuration file from the router to a server using FTP, the Cisco IOS software sends the first valid username it encounters in the following list:

1. The username specified in the **copy** command, if a username is specified.
2. The username set by the **ip ftp username** global configuration command, if the command is configured.
3. Anonymous.

The router sends the first valid password it encounters in the following list:

1. The password specified in the **copy** command, if a password is specified.
2. The password set by the **ip ftp password** global configuration command, if the command is configured.
3. A password *username@routename.domain* formed by the router. The variable *username* is the username associated with the current session, *routename* is the configured host name, and *domain* is the domain of the router.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user on the router.

If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the username on the server. For example, if the system image resides in the home directory of a user on the server, specify the name of that user as the remote username.

Refer to the documentation for your FTP server for more details.

Use the **ip ftp username** and **ip ftp password** commands to specify a username and password for all copies. Include the username in the **copy** command if you want to specify a username for that copy operation only.

Storing Images on Servers

Use the **copy flash: destination-url** command (for example, **copy flash: tftp:**) to copy a system image or boot image from Flash memory to a network server. Use the copy of the image as a backup copy. Also, use it to verify that the copy in Flash memory is the same as that in the original file.

Copying from a Server to Flash Memory

Use the **copy destination-url flash:** command (for example, **copy tftp: flash:**) to copy an image from a server to Flash memory.

On Class B file system platforms, the system provides an option to erase existing Flash memory before writing onto it.



Caution

Verify the image in Flash memory before booting the image.

Verifying Images

Before booting from Flash memory, verify that the checksum of the image in Flash memory matches the checksum listed in the README file that was distributed with the image by using the **verify EXEC** command. The checksum of the image in Flash memory is displayed when the **copy** command completes copying the image. The README file was copied to the server automatically when you installed the image.



Caution

If the checksum values do not match, do not reboot the router. Instead, reissue the **copy** command and compare the checksums again. If the checksum is repeatedly wrong, copy the original image back into Flash memory *before* you reboot the router from Flash memory. If you have a corrupted image in Flash memory and try to boot from Flash memory, the router will start the system image contained in ROM (assuming that booting from a network server is not configured). If ROM does not contain a fully functional system image, the router might not function and will need to be reconfigured through a direct console port connection.

Copying a Configuration File from a Server to the Running Configuration

Use the **copy {ftp: | rcp: | tftp:} running-config** command to load a configuration file from a network server to the running configuration of the router (note that **running-config** is the alias for the **system:running-config** keyword). The configuration will be added to the running configuration as if the commands were typed in the command-line interface. Thus, the resulting configuration file will be a combination of the previous running configuration and the loaded configuration file, with the loaded configuration file having precedence.

You can copy either a host configuration file or a network configuration file. Accept the default value of *host* to copy and load a host configuration file containing commands that apply to one network server in particular. Enter *network* to copy and load a network configuration file containing commands that apply to all network servers on a network.

Copying a Configuration File from a Server to the Startup Configuration

Use the **copy {ftp: | rcp: | tftp:} nvram:startup-config** command to copy a configuration file from a network server to the startup configuration of the router. These commands replace the startup configuration file with the copied configuration file.

Storing the Running or Startup Configuration on a Server

Use the **copy system:running-config {ftp: | rcp: | tftp:}** command to copy the current configuration file to a network server using FTP, rcp, or TFTP. Use the **copy nvram:startup-config {ftp: | rcp: | tftp:}** command to copy the startup configuration file to a network server.

The configuration file copy can serve as a backup copy.

Saving the Running Configuration to the Startup Configuration

Use the **copy system:running-config nvram:startup-config** command to copy the running configuration to the startup configuration.



Caution

Some specific commands may not get saved to NVRAM. You will need to enter these commands again if you reboot the machine. We recommend that you keep a listing of these settings so you can quickly reconfigure your router after rebooting.

If you issue the **copy system:running-config nvram:startup-config** command from a bootstrap system image, a warning will instruct you to indicate whether you want your previous NVRAM configuration to be overwritten and configuration commands to be lost. This warning does not appear if NVRAM contains an invalid configuration or if the previous configuration in NVRAM was generated by a bootstrap system image.

On all platforms except Class A file system platforms, the **copy system:running-config nvram:startup-config** command copies the currently running configuration to NVRAM.

On the Class A Flash file system platforms, the **copy system:running-config nvram:startup-config** command copies the currently running configuration to the location specified by the CONFIG_FILE environment variable. This variable specifies the device and configuration file used for initialization. When the CONFIG_FILE environment variable points to NVRAM or when this variable does not exist (such as at first-time startup), the Cisco IOS software writes the current configuration to NVRAM. If the current configuration is too large for NVRAM, the software displays a message and stops executing the command.

When the CONFIG_FILE environment variable specifies a valid device other than **nvram:** (that is, **flash:**, **bootflash:**, **slot0:**, or **slot1:**), the software writes the current configuration to the specified device and filename and stores a distilled version of the configuration in NVRAM. A distilled version is one that does not contain access list information. If NVRAM already contains a copy of a complete configuration, the router prompts you to confirm the copy.

Using CONFIG_FILE, BOOTLDR, and BOOT Environment Variables

Class A Flash file system platforms have the following features:

- The CONFIG_FILE environment variable specifies the configuration file used during router initialization.
- The BOOTLDR environment variable specifies the Flash device and filename containing the boot helper image (rxboot) that ROM uses for booting.
- The BOOT environment variable specifies a list of bootable images on various devices.
- Cisco 3600 routers do not use a dedicated rxboot, which many other routers use to help with the boot process. Instead, the BOOTLDR ROM monitor environment variable identifies the Flash memory device and filename that are used as the boot helper; the default is the first system image in Flash memory.
- The BOOT environment variable specifies a list of bootable images on various devices.

To display the contents of environment variables, use the **show bootvar** command in EXEC mode. To modify the CONFIG_FILE environment variable, use the **boot config** global configuration command. To modify the BOOTLDR environment variable, use the **boot bootldr** global configuration command. To modify the BOOT environment variable, use the **boot system** global configuration command. To save your modifications, use the **copy system:running-config nvram:startup-config** command.

When the destination of a **copy** command is specified by the CONFIG_FILE or BOOTLDR environment variable, the router prompts you for confirmation before proceeding with the copy. When the destination is the only valid image in the BOOT environment variable, the router also prompts you for confirmation before proceeding with the copy.

Using the copy Command with HSA

HSA is the feature that allows you to install two RSP cards in a single router on the Cisco 7507 and Cisco 7513 platforms.

On a Cisco 7507 or Cisco 7513 router configured for HSA, if you copy a file to **nvramp:startup-configuration** with automatic synchronization disabled, the system asks if you also want to copy the file to the startup configuration of the slave. The default answer is **yes**. If automatic synchronization is enabled, the system automatically copies the file to the startup configuration of the slave each time you use a **copy** command with **nvramp:startup-configuration** as the destination.

Examples

The following examples show uses of the **copy** command. Depending on your platform, the output might be different from that shown in the examples.

- Copy an Image from a Server to Flash Memory Examples
- Save a Copy of an Image on a Server Examples
- Copy from a Server to the Running Configuration Example
- Copy from a Server to the Startup Configuration Example
- Copy the Running Configuration to a Server Example
- Copy the Startup Configuration to a Server Example
- Save the Current Running Configuration Example
- Move Configuration Files to Other Locations Examples
- Copy an Image from the Master RSP Card to the Slave RSP Card Example

Copy an Image from a Server to Flash Memory Examples

The following three examples use **copy rcp:**, **copy tftp:**, and **copy ftp:** commands to copy an image from a server to Flash memory.

Copy an Image from a Server to Flash Memory Example

The following example copies a system image named file1 from the remote rcp server with an IP address of 172.16.101.101 to Flash memory. On Class B file system platforms, the Cisco IOS software allows you to first erase the contents of Flash memory to ensure that enough Flash memory is available to accommodate the system image.

```
Router# copy rcp://netadmin@172.16.101.101/file1 flash:file1

Destination file name [file1]?
Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101 (via Ethernet0): ! [OK]

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy 'file1' from server
  as 'file1' into Flash WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee...erased
Loading file1 from 172.16.101.101 (via Ethernet0): !
[OK - 984/8388608 bytes]

Verifying checksum... OK (0x14B3)
Flash copy took 0:00:01 [hh:mm:ss]
```

Copy from a Server to a Flash Memory Using Flash Load Helper Example

The following example copies a system image into a partition of Flash memory. The system will prompt for a partition number only if there are two or more read/write partitions or one read-only and one read/write partition and dual Flash bank support in boot ROMs. If the partition entered is not valid, the

process terminates. You can enter a partition number, a question mark (?) for a directory display of all partitions, or a question mark and a number (?*number*) for directory display of a particular partition. The default is the first read/write partition. In this case, the partition is read-only and has dual Flash bank support in boot ROM, so the system uses Flash Load Helper.

```
Router# copy tftp: flash:
```

```
System flash partition information:
```

| Partition | Size | Used | Free | Bank-Size | State | Copy-Mode |
|-----------|-------|-------|-------|-----------|------------|------------|
| 1 | 4096K | 2048K | 2048K | 2048K | Read Only | RXBOOT-FLH |
| 2 | 4096K | 2048K | 2048K | 2048K | Read/Write | Direct |

```
[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 2]
```

```
**** NOTICE ****
```

```
Flash load helper v1.0
```

```
This process will accept the copy options and then terminate
the current system image to use the ROM based image for the copy.
Routing functionality will not be available during that time.
If you are logged in via telnet, this connection will terminate.
Users with console access can see the results of the copy operation.
```

```
---- ***** ----
```

```
Proceed? [confirm]
```

```
System flash directory, partition 1:
```

```
File Length Name/status
```

```
1 3459720 master/igs-bfpx.100-4.3
```

```
[3459784 bytes used, 734520 available, 4194304 total]
```

```
Address or name of remote host [255.255.255.255]? 172.16.1.1
```

```
Source file name? master/igs-bfpx-100.4.3
```

```
Destination file name [default = source name]?
```

```
Loading master/igs-bfpx.100-4.3 from 172.16.1.111: !
```

```
Erase flash device before writing? [confirm]
```

```
Flash contains files. Are you sure? [confirm]
```

```
Copy 'master/igs-bfpx.100-4.3' from TFTP server
```

```
as 'master/igs-bfpx.100-4.3' into Flash WITH erase? [yes/no] yes
```

In addition to an IP address such as 172.16.1.1, an IPv6 address such as [2001:0DB8::2] is acceptable to the system.

Copy an Image from a Server to a Flash Memory Card Partition Example

The following example copies the file c3600-i-mz from the rcp server at IP address 172.23.1.129 to the Flash memory card in slot 0 of a Cisco 3600 series router, which has only one partition. As the operation progresses, the Cisco IOS software asks you to erase the files on the Flash memory PC card to accommodate the incoming file. This entire operation takes 18 seconds to perform, as indicated at the end of the example.

```
Router# copy rcp: slot0:
```

```
PCMCIA Slot0 flash
```

| Partition | Size | Used | Free | Bank-Size | State | Copy Mode |
|-----------|-------|-------|-------|-----------|------------|-----------|
| 1 | 4096K | 3068K | 1027K | 4096K | Read/Write | Direct |
| 2 | 4096K | 1671K | 2424K | 4096K | Read/Write | Direct |
| 3 | 4096K | 0K | 4095K | 4096K | Read/Write | Direct |
| 4 | 4096K | 3825K | 270K | 4096K | Read/Write | Direct |

```
[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 1]
```

```
PCMCIA Slot0 flash directory, partition 1:
```

```

File Length Name/status
  1 3142288 c3600-j-mz.test
[3142352 bytes used, 1051952 available, 4194304 total]
Address or name of remote host [172.23.1.129]?
Source file name? /tftpboot/images/c3600-i-mz
Destination file name [/tftpboot/images/c3600-i-mz]?
Accessing file '/tftpboot/images/c3600-i-mz' on 172.23.1.129...
Connected to 172.23.1.129
Loading 1711088 byte file c3600-i-mz: ! [OK]

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy '/tftpboot/images/c3600-i-mz' from server
  as '/tftpboot/images/c3600-i-mz' into Flash WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Connected to 172.23.1.129
Loading 1711088 byte file c3600-i-mz:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Verifying checksum... OK (0xF89A)
Flash device copy took 00:00:18 [hh:mm:ss]

```

Save a Copy of an Image on a Server Examples

The following four examples use **copy** commands to copy images to a server for storage.

Copy an Image from Flash Memory to an rcp Server Example

The following example copies a system image from Flash memory to an rcp server using the default remote username. Because the rcp server address and filename are not included in the command, the router prompts for it.

```

Router# copy flash: rcp:

IP address of remote host [255.255.255.255]? 172.16.13.110
Name of file to copy? gsxx
writing gsxx - copy complete

```

Copy an Image from a Partition of Flash Memory to a Server Example

The following example copies an image from a particular partition of Flash memory to an rcp server using a remote username of netadmin1.

The system will prompt if there are two or more partitions. If the partition entered is not valid, the process terminates. You have the option to enter a partition number, a question mark (?) for a directory display of all partitions, or a question mark and a number (?number) for a directory display of a particular partition. The default is the first partition.

```

Router# configure terminal
Router# ip rcmd remote-username netadmin1
Router# end
Router# copy flash: rcp:

System flash partition information:
Partition  Size    Used    Free    Bank-Size    State    Copy-Mode
    1      4096K    2048K    2048K    2048K        Read Only    RXBOOT-FLH
    2      4096K    2048K    2048K    2048K    Read/Write    Direct
[Type ?<number> for partition directory; ? for full directory; q to abort]
Which partition? [1] 2

System flash directory, partition 2:

```

```

File Length Name/status
  1 3459720 master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]
Address or name of remote host [ABC.CISCO.COM]?
Source file name? master/igs-bfpx.100-4.3
Destination file name [master/igs-bfpx.100-4.3]?
Verifying checksum for 'master/igs-bfpx.100-4.3' (file # 1)... OK
Copy 'master/igs-bfpx.100-4.3' from Flash to server
as 'master/igs-bfpx.100-4.3'? [yes/no] yes
!!!!...
Upload to server done
Flash copy took 0:00:00 [hh:mm:ss]

```

Copy an Image from a Flash Memory File System to an FTP Server

The following example copies the file c3600-i-mz from partition 1 of the Flash memory card in slot 0 to an FTP server at IP address 172.23.1.129.

```

Router# show slot0: partition 1

PCMCIA Slot0 flash directory, partition 1:
File Length Name/status
  1 1711088 c3600-i-mz
[1711152 bytes used, 2483152 available, 4194304 total]

Router# copy slot0:1:c3600-i-mz ftp://myuser:mypass@172.23.1.129/c3600-i-mz
Verifying checksum for '/tftpboot/cisco_rules/c3600-i-mz' (file # 1)... OK
Copy '/tftpboot/cisco_rules/c3600-i-mz' from Flash to server
as 'c3700-i-mz'? [yes/no] yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upload to server done
Flash device copy took 00:00:23 [hh:mm:ss]

```

Copy an Image from Boot Flash Memory to a TFTP Server

The following example copies an image from boot flash memory to a TFTP server:

```

Router# copy bootflash:file1 tftp://192.168.117.23/file1

Verifying checksum for 'file1' (file # 1)... OK
Copy 'file1' from Flash to server
as 'file1'? [yes/no] y
!!!!...
Upload to server done
Flash copy took 0:00:00 [hh:mm:ss]

```

If the TFTP server in this example has an IPv6 address of 2001:0DB8::2, you can specify the following command:

```

Router# copy bootflash:file1 tftp://[2001:0DB8::2]/file1

```

Copy from a Server to the Running Configuration Example

The following example copies and runs a configuration file named host1-confg from the netadmin1 directory on the remote server with an IP address of 172.16.101.101:

```

Router# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config

Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Router#

```

```
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

Copy from a Server to the Startup Configuration Example

The following example copies a configuration file named host2-config from a remote FTP server to the startup configuration. The IP address is 172.16.101.101, the remote username is netadmin1, and the remote password is ftppass.

```
Router# copy ftp://netadmin1:ftppass@172.16.101.101/host2-config nvram:startup-config
```

```
Configure using rtr2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file rtr2-config:[OK]
[OK]
Router#
%SYS-5-CONFIG_NV:Non-volatile store configured from rtr2-config by
FTP from 172.16.101.101
```

Copy the Running Configuration to a Server Example

The following example specifies a remote username of netadmin1. Then it copies the running configuration file named Rtr2-config to the netadmin1 directory on the remote host with an IP address of 172.16.101.101.

```
Router# configure terminal
Router(config)# ip rcmd remote-username netadmin1
Router(config)# end
Router# copy system:running-config rcp:
Remote host []? 172.16.101.101

Name of configuration file to write [Rtr2-config]?
Write file rtr2-config on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
```

Copy the Startup Configuration to a Server Example

The following example copies the startup configuration to a TFTP server:

```
Router# copy nvram:startup-config tftp:
Remote host []? 172.16.101.101

Name of configuration file to write [rtr2-config]? <cr>
Write file rtr2-config on host 172.16.101.101?[confirm] <cr>
! [OK]
```

In addition to an IP address such as 172.16.101.101, an IPv6 address such as [2001:0DB8::2] is acceptable to the system.

Save the Current Running Configuration Example

The following example copies the running configuration to the startup configuration. On a Class A Flash file system platform, this command copies the running configuration to the startup configuration specified by the CONFIG_FILE environment variable.

```
copy system:running-config nvram:startup-config
```

The following example shows the warning the system provides if you try to save configuration information from bootstrap into the system:

```
Router(boot)# copy system:running-config nvram:startup-config
```

```
Warning: Attempting to overwrite an NVRAM configuration written
by a full system image. This bootstrap software does not support
```

the full configuration command set. If you perform this command now, some configuration commands may be lost.
 Overwrite the previous NVRAM configuration? [confirm]

Enter **no** to escape writing the configuration information to memory.

Move Configuration Files to Other Locations Examples

On some routers, you can store copies of configuration files on a Flash memory device. Five examples follow.

Copy the Startup Configuration to a Flash Memory Device Example

The following example copies the startup configuration file (specified by the CONFIG_FILE environment variable) to a Flash memory card inserted in slot 0:

```
Router# copy nvram:startup-config slot0:router-config
```

Copy the Running Configuration to a Flash Memory Device Example

The following example copies the running configuration from the router to the Flash memory PC card in slot 0:

```
Router# copy system:running-config slot0:cisco
```

```
Building configuration...
```

```
5267 bytes copied in 0.720 secs
```

Copy to the Running Configuration from a Flash Memory Device Example

The following example copies the file named ios-upgrade-1 from the Flash memory card in slot 0 to the running configuration:

```
Router# copy slot0:4:ios-upgrade-1 system:running-config
```

```
Copy 'ios-upgrade-1' from flash device
as 'running-config' ? [yes/no] yes
```

Copy to the Startup Configuration from a Flash Memory Device Example

The following example copies the file named router-image from the Flash memory to the startup configuration:

```
Router# copy flash:router-image nvram:startup-config
```

Copy a Configuration File from a Flash Device to Another Example

The following example copies the file named running-config from the first partition in internal Flash memory to the Flash memory PC card in slot 1. The checksum of the file is verified, and its copying time of 30 seconds is displayed.

```
Router# copy flash: slot1:
```

```
System flash
```

| Partition | Size | Used | Free | Bank-Size | State | Copy Mode |
|-----------|--------|-------|--------|-----------|------------|-----------|
| 1 | 4096K | 3070K | 1025K | 4096K | Read/Write | Direct |
| 2 | 16384K | 1671K | 14712K | 8192K | Read/Write | Direct |

```
[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 1]
```

```
System flash directory, partition 1:
```



```

File Length Name/status
  1 3142748 server1/images/server2/c3600-j-mz.latest
  2 850 running-config
[3143728 bytes used, 1050576 available, 4194304 total]

PCMCIA Slot1 flash directory:
File Length Name/status
  1 1711088 server3/images/c3600-i-mz
  2 850 running-config
[1712068 bytes used, 2482236 available, 4194304 total]
Source file name? running-config
Destination file name [running-config]?
Verifying checksum for 'running-config' (file # 2)... OK
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy 'running-config' from flash: device
as 'running-config' into slot1: device WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
!
[OK - 850/4194304 bytes]

Flash device copy took 00:00:30 [hh:mm:ss]
Verifying checksum... OK (0x16)

```

Copy an Image from the Master RSP Card to the Slave RSP Card Example

The following example copies the file named router-image from the Flash memory card inserted in slot 1 of the master RSP card to slot 0 of the slave RSP card in the same router:

```
copy slot1:router-image slaveslot0:
```

| Related Commands | Command | Description |
|------------------|------------------------------------|--|
| | boot config | Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup). This command is available only on Class A file system platforms. |
| | boot system | Specifies the system image that the router loads at startup. |
| | cd | Changes the default directory or file system. |
| | copy xmodem: flash: | Copies a Cisco IOS image from a local or remote computer to Flash memory on a Cisco router using the Xmodem protocol. |
| | copy ymodem: flash: | Copies a Cisco IOS image from a local or remote computer to Flash memory on a Cisco router using the Ymodem protocol. |
| | delete | Deletes a file on a Flash memory device. |
| | dir | Displays a list of files on a file system. |
| | erase | Erases a file system. |
| | ip rcmd remote-username | Configures the remote username to be used when requesting a remote copy using rcp. |
| | reload | Reloads the operating system. |
| | show bootvar | Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting. |
| | show file systems | Displays the layout and contents of a Flash memory file system. |

| Command | Description |
|-------------------------------|--|
| slave auto-sync config | Turns on automatic synchronization of configuration files for a Cisco 7507 or Cisco 7513 router that is configured for HSA. |
| verify bootflash: | Verifies the checksum of a file on a Flash memory file system (including boot flash). Either of the identical verify bootflash: or verify bootflash commands replaces the copy verify bootflash command. Refer to the verify command for more information. |

debug bgp ipv6 dampening

To display debugging messages for IPv6 Border Gateway Protocol (BGP) dampening, use the **debug bgp ipv6 dampening** command in privileged EXEC mode. To disable debugging messages for IPv6 BGP dampening, use the **no** form of this command.

debug bgp ipv6 dampening [**prefix-list** *prefix-list-name*]

no debug bgp ipv6 dampening [**prefix-list** *prefix-list-name*]

Syntax Description

prefix-list *prefix-list-name* (Optional) Name of an IPv6 prefix list.

Defaults

Debugging for IPv6 BGP dampening packets is not enabled.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|----------------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(13)T, 12.0(24)S | The prefix-list keyword was added. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

The **debug bgp ipv6 dampening** command is similar to the **debug ip bgp dampening** command, except that it is IPv6-specific.

Use the **prefix-list** keyword and an argument to filter BGP IPv6 dampening debug information through an IPv6 prefix list.



Note

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debugging output, use the logging command options within global configuration mode. Destinations are the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debugging output, refer to the *Cisco IOS Debug Command Reference*.

Examples

The following is sample output from the **debug bgp ipv6 dampening** command:

```
Router# debug bgp ipv6 dampening
```

```
00:13:28:BGP(1):charge penalty for 2000:0:0:1::/64 path 2 1 with halflife-time 15
reuse/suppress 750/2000
```

```

00:13:28:BGP(1):flapped 1 times since 00:00:00. New penalty is 1000
00:13:28:BGP(1):charge penalty for 2000:0:0:1:1::/80 path 2 1 with halflife-time 15
reuse/suppress 750/2000
00:13:28:BGP(1):flapped 1 times since 00:00:00. New penalty is 1000
00:13:28:BGP(1):charge penalty for 2000:0:0:5::/64 path 2 1 with halflife-time 15
reuse/suppress 750/2000
00:13:28:BGP(1):flapped 1 times since 00:00:00. New penalty is 1000
00:16:03:BGP(1):charge penalty for 2000:0:0:1:1::/64 path 2 1 with halflife-time 15
reuse/suppress 750/2000
00:16:03:BGP(1):flapped 2 times since 00:02:35. New penalty is 1892

00:18:28:BGP(1):suppress 2000:0:0:1:1::/80 path 2 1 for 00:27:30 (penalty 2671)
00:18:28:halflife-time 15, reuse/suppress 750/2000
00:18:28:BGP(1):suppress 2000:0:0:1:1::/64 path 2 1 for 00:27:20 (penalty 2664)
00:18:28:halflife-time 15, reuse/suppress 750/2000

```

The following example shows output for the **debug bgp ipv6 dampening** command filtered through the prefix list named marketing:

```
Router# debug bgp ipv6 dampening prefix-list marketing
```

```

00:16:08:BGP(1):charge penalty for 2001:0DB8::/64 path 30 with halflife-time 15
reuse/suppress 750/2000
00:16:08:BGP(1):flapped 1 times since 00:00:00. New penalty is 10

```

Table 6 describes the fields shown in the display.

Table 6 *debug bgp ipv6 dampening Field Descriptions*

| Field | Description |
|--|---|
| penalty | Numerical value of 1000 assigned to a route by a router configured for route dampening in another autonomous system each time a route flaps. Penalties are cumulative. The penalty for the route is stored in the BGP routing table until the penalty exceeds the suppress limit. If the penalty exceeds the suppress limit, the route state changes from history to damp. |
| flapped | Number of times a route is available, then unavailable, or vice versa. |
| halflife-time | Amount of time (in minutes) by which the penalty is decreased after the route is assigned a penalty. The halflife-time value is half of the half-life period (which is 15 minutes by default). Penalty reduction happens every 5 seconds. |
| reuse | The limit by which a route is unsuppressed. If the penalty for a flapping route decreases and falls below this reuse limit, the route is unsuppressed. That is, the route is added back to the BGP table and once again used for forwarding. The default reuse limit is 750. Routes are unsuppressed at 10-second increments. Every 10 seconds, the router determines which routes are now unsuppressed and advertises them to the world. |
| suppress | Limit by which a route is suppressed. If the penalty exceeds this limit, the route is suppressed. The default value is 2000. |
| maximum suppress limit (not shown in sample output) | Maximum amount of time (in minutes) a route is suppressed. The default value is four times the half-life period. |
| damp state (not shown in sample output) | State in which the route has flapped so often that the router will not advertise this route to BGP neighbors. |

Related Commands

| Command | Description |
|-------------------------------|--|
| debug bgp ipv6 updates | Displays debugging messages for IPv6 BGP update packets. |

debug bgp ipv6 updates

To display debugging messages for IPv6 Border Gateway Protocol (BGP) update packets, use the **debug bgp ipv6 updates** command in privileged EXEC mode. To disable debugging messages for IPv6 BGP update packets, use the **no** form of this command.

debug bgp ipv6 updates [*ipv6-address*] [**prefix-list** *prefix-list-name*] [**in** | **out**]

no debug bgp ipv6 updates [*ipv6-address*] [**prefix-list** *prefix-list-name*] [**in** | **out**]

| | | |
|--------------------|--|--|
| Syntax Description | ipv6-address | (Optional) The IPv6 address of a BGP neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| | prefix-list <i>prefix-list-name</i> | (Optional) Name of an IPv6 prefix list. |
| | in | (Optional) Indicates inbound updates. |
| | out | (Optional) Indicates outbound updates. |
| | | |

Defaults Debugging for IPv6 BGP update packets is not enabled.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|----------------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(13)T, 12.0(24)S | The prefix-list keyword was added. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines The **debug bgp ipv6 updates** command is similar to the **debug ip bgp updates** command, except that it is IPv6-specific.

Use the **prefix-list** keyword to filter BGP IPv6 updates debugging information through an IPv6 prefix list.



Note

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debugging output, use the logging command options within global configuration mode. Destinations are the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debugging output, refer to the Release 12.2 *Cisco IOS Debug Command Reference*.

Examples

The following is sample output from the **debug bgp ipv6 updates** command:

```
Router# debug bgp ipv6 updates
```

```
14:04:17:BGP(1):2000:0:0:2::2 computing updates, afi 1, neighbor version 0, table version
1, starting at ::
14:04:17:BGP(1):2000:0:0:2::2 update run completed, afi 1, ran for 0ms, neighbor version
0, start version 1, throttled to 1
14:04:19:BGP(1):sourced route for 2000:0:0:2::1/64 path #0 changed (weight 32768)
14:04:19:BGP(1):2000:0:0:2::1/64 route sourced locally
14:04:19:BGP(1):2000:0:0:2:1::/80 route sourced locally
14:04:19:BGP(1):2000:0:0:3::2/64 route sourced locally
14:04:19:BGP(1):2000:0:0:4::2/64 route sourced locally
14:04:22:BGP(1):2000:0:0:2::2 computing updates, afi 1, neighbor version 1, table version
6, starting at ::
14:04:22:BGP(1):2000:0:0:2::2 send UPDATE (format) 2000:0:0:2::1/64, next 2000:0:0:2::1,
metric 0, path
14:04:22:BGP(1):2000:0:0:2::2 send UPDATE (format) 2000:0:0:2:1::/80, next 2000:0:0:2::1,
metric 0, path
14:04:22:BGP(1):2000:0:0:2::2 send UPDATE (prepend, chgflags:0x208) 2000:0:0:3::2/64, next
2000:0:0:2::1, metric 0, path
14:04:22:BGP(1):2000:0:0:2::2 send UPDATE (prepend, chgflags:0x208) 2000:0:0:4::2/64, next
2000:0:0:2::1, metric 0, path
```

The following is sample output from the **debug bgp ipv6 updates** command filtered through the prefix list named sales:

```
Router# debug bgp ipv6 updates prefix-list sales
```

```
00:18:26:BGP(1):2000:8493:1::2 send UPDATE (prepend, chgflags:0x208) 7878:7878::/64, next
2001:0DB8::36C, metric 0, path
```

Table 7 describes the significant fields shown in the display.

Table 7 *debug bgp ipv6 updates Field Descriptions*

| Field | Description |
|---------------------------------------|--|
| BGP(1): | BGP debugging for address family index (afi) 1. |
| afi | Address family index. |
| neighbor version | Version of the BGP table on the neighbor from which the update was received. |
| table version | Version of the BGP table on the router from which you entered the debug bgp ipv6 updates command. |
| starting at | Starting at the network layer reachability information (NLRI). BGP sends routing update messages containing NLRI to describe a route and how to get there. In this context, an NLRI is a prefix. A BGP update message carries one or more NLRI prefixes and the attributes of a route for the NLRI prefixes; the route attributes include a BGP next hop gateway address, community values, and other information. |
| route sourced locally | Indicates that a route is sourced locally and that updates are not sent for the route. |
| send UPDATE (format) | Indicates that an update message for a reachable network should be formatted. Addresses include prefix and next hop. |
| send UPDATE (prepend, chgflags:0x208) | Indicates that an update message about a path to a BGP peer should be written. |

Related Commands

| Command | Description |
|--------------------------|---|
| debug bgp ipv6 dampening | Displays debugging messages for IPv6 BGP dampening packets. |

debug crypto ipv6 ipsec

To display IP Security (IPSec) events for IPv6 networks, use the **debug crypto ipv6 ipsec** command. To disable debug messages for IPSec for IPv6 networks, use the **no** form of this command.

debug crypto ipv6 ipsec

no debug crypto ipv6 ipsec

Syntax Description This command has no arguments or keywords.

Defaults Debugging for IPv6 IPSec events is not enabled.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.3(4)T | This command was introduced. |

Usage Guidelines Use this command to display IPSec events while setting up or removing policy definitions during OSPF configuration.

| Related Commands | Command | Description |
|------------------|---------------------------------------|---|
| | debug crypto engine | Displays debugging messages about crypto engines, which perform encryption and decryption. |
| | debug crypto ipv6 packet | Displays debug messages for IPv6 packets allowing you to see the contents of packets outbound from a Cisco router when the remote node is not a Cisco node. |
| | debug crypto socket | Displays communication between the client and IPSec during policy setup and removal processes. |
| | debug ipv6 ospf authentication | Shows the interaction between OSPF and IPSec, including creation or removal of policies. |

debug crypto ipv6 packet

To display the contents of IPv6 packets, use the **debug crypto ipv6 packet** command. To disable debug messages for IPv6 packets, use the **no** form of this command.

debug crypto ipv6 packet

no debug crypto ipv6 packet

Syntax Description This command has no arguments or keywords.

Defaults Debugging for IPv6 IPsec packets is not enabled.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.3(4)T | This command was introduced. |

Usage Guidelines Consult Cisco Technical Support before using this command.

Use this command to display the contents of IPv6 packets. This command is useful when the remote node is not a Cisco device and communication between the Cisco and non-Cisco router cannot be established. This command enable you to look at the contents of the packets outbound from the Cisco router.


Caution

This command examines the content of every IPv6 packet and will affect network performance.

Examples This example shows the ouptut of each packet when the **debug crypto ipv6 packet** command is enabled.

```
Router# debug crypto ipv6 packet
Crypto IPv6 IPSEC packet debugging is on

Router#
*Oct 30 16:57:06.330:
IPSECv6:before Encapsulation of IPv6 packet:
0E37A7C0:                6E000000 00285901                n....(Y.
0E37A7D0:FE800000 00000000 020A8BFF FED42C1D ~.....~T,.
0E37A7E0:FF020000 00000000 00000000 00000005 .....
0E37A7F0:03010028 01010104 00000001 8AD80000 ..(.....X..
0E37A800:00000006 01000013 000A0028 0A0250CF .....(..PO
0E37A810:01010104 0A0250CF                .....PO
*Oct 30 16:57:06.330:
IPSECv6:Encapsulated IPv6 packet
:
0E37A7B0:6E000000 00403301 FE800000 00000000 n....@3.~.....
0E37A7C0:020A8BFF FED42C1D FF020000 00000000 ....~T,.....
0E37A7D0:00000000 00000005 59040000 000022B8 .....Y....."8
```

```

0E37A7E0:0000001A 38AB1ED8 04C1C6FB FF1248CF ....8+.X.AF{..HO
0E37A7F0:03010028 01010104 00000001 8AD80000 ... (.....X..
0E37A800:00000006 01000013 000A0028 0A0250CF ..... (..PO
0E37A810:01010104 0A0250CF .....PO
*Oct 30 16:57:11.914:
IPSECv6:Before Decapsulation of IPv6 packet
:
0E004A50:                6E000000 00403301                n....@3.
0E004A60:FE800000 00000000 023071FF FE7FE81D ~.....0q.~.h.
0E004A70:FF020000 00000000 00000000 00000005 .....
0E004A80:59040000 000022B8 00001D88 F5AC68EE Y....."8....u,hn
0E004A90:1AC00088 947C6BF2 03010028 0A0250CF .@...|kr... (..PO
0E004AA0:00000001 E9080000 00000004 01000013 ....i.....
0E004AB0:000A0028 0A0250CF 01010104 01010104 ... (..PO.....
0E004AC0:
*Oct 30 16:57:11.914:
IPSECv6:Decapsulated IPv6 packet
:
0E004A70:6E000000 00285901 FE800000 00000000 n....(Y.~.....
0E004A80:023071FF FE7FE81D FF020000 00000000 .0q.~.h.....
0E004A90:00000000 00000005 03010028 0A0250CF ..... (..PO
0E004AA0:00000001 E9080000 00000004 01000013 ....i.....
0E004AB0:000A0028 0A0250CF 01010104 01010104 ... (..PO.....
0E004AC0:
*Oct 30 16:57:16.330:
IPSECv6:before Encapsulation of IPv6 packet:
0E003DC0:                6E000000 00285901                n....(Y.
0E003DD0:FE800000 00000000 020A8BFF FED42C1D ~.....~T,.
0E003DE0:FF020000 00000000 00000000 00000005 .....
0E003DF0:03010028 01010104 00000001 8AD80000 ... (.....X..
0E003E00:00000006 01000013 000A0028 0A0250CF ..... (..PO
0E003E10:01010104 0A0250CF .....PO
*Oct 30 16:57:16.330:
IPSECv6:Encapsulated IPv6 packet
:
0E003DB0:6E000000 00403301 FE800000 00000000 n....@3.~.....
0E003DC0:020A8BFF FED42C1D FF020000 00000000 ....~T,.....
0E003DD0:00000000 00000005 59040000 000022B8 .....Y....."8
0E003DE0:0000001B F8E3C4E2 4CC4B690 DDF32B5C ...xcDbLD6.]s\
0E003DF0:03010028 01010104 00000001 8AD80000 ... (.....X..
0E003E00:00000006 01000013 000A0028 0A0250CF ..... (..PO
0E003E10:01010104 0A0250CF .....PO

```

Related Commands

| Command | Description |
|---------------------------------------|--|
| debug crypto engine | Displays debugging messages about crypto engines, which perform encryption and decryption. |
| debug crypto ipv6 ipsec | Displays IP Security (IPSec) events for IPv6 networks. |
| debug crypto socket | Displays communication between the client and IPSec during policy setup and removal processes. |
| debug ipv6 ospf authentication | Shows the interaction between OSPF and IPSec, including creation or removal of policies. |

debug ipv6 cef drop

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) dropped packets, use the **debug ipv6 cef drop** command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 dropped packets, use the **no** form of this command.

debug ipv6 cef drop

no debug ipv6 cef drop

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging for CEFv6 and dCEFv6 dropped packets is not enabled.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.0(22)S | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **debug ipv6 cef drop** command is similar to the **debug ip cef drops** command, except that it is IPv6-specific.



Note

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on **debug** commands and redirecting debug output, refer to the Release 12 *Cisco IOS Debug Command Reference*.

Examples

The following is sample output from the **debug ipv6 cef drop** command:

```
Router# debug ipv6 cef drop
```

```
*Aug 30 08:20:51.169: IPv6-CEF: received packet on Serial6/0/2
*Aug 30 08:20:51.169: IPv6-CEF: found no adjacency for 2001:0DB8::1 reason 2
*Aug 30 08:20:51.169: IPv6-CEF: packet not switched: code 0x1
```

Table 8 describes the significant fields shown in the display.

Table 8 *debug ipv6 cef drop Field Descriptions*

| Field | Description |
|---|---|
| IPv6-CEF: received packet on Serial6/0/2 | CEF has received a packet addressed to the router via serial interface 6/0/2. |
| IPv6-CEF: found no adjacency for 2001:0DB8::1 | CEF has found no adjacency for the IPv6 address prefix of 2001:0DB8::1. |
| IPv6-CEF: packet not switched | CEF has dropped the packet. |

Related Commands

| Command | Description |
|------------------------------|---|
| debug ipv6 cef events | Displays debug messages for CEFv6 and dCEFv6 general events. |
| debug ipv6 cef table | Displays debug messages for CEFv6 and dCEFv6 table modification events. |

debug ipv6 cef events

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) general events, use the **debug ipv6 cef events** command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 general events, use the **no** form of this command.

debug ipv6 cef events

no debug ipv6 cef events

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging for CEFv6 and dCEFv6 general events is not enabled.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.0(22)S | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **debug ipv6 cef events** command is similar to the **debug ip cef events** command, except that it is IPv6-specific.



Note

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on **debug** commands and redirecting debug output, refer to the Release 12 *Cisco IOS Debug Command Reference*.

Examples

The following is sample output from the **debug ipv6 cef events** command:

```
Router# debug ipv6 cef events
```

```
IPv6 CEF packet events debugging is on
```

```
Router#
```

```
*Aug 30 08:22:57.809: %LINK-3-UPDOWN: Interface Serial6/0/2, changed state to up
```

```
*Aug 30 08:22:58.809: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial6/0/2, changed state to up
```

```
*Aug 30 08:23:00.821: CEFv6-IDB: Serial6/0/2 address 2001:0DB8::248 add download succeeded
```

Table 9 describes the significant fields shown in the display.

Table 9 *debug ipv6 cef events Field Descriptions*

| Field | Description |
|---|--|
| Interface Serial6/0/2, changed state to up | Indicates that the interface hardware on serial interface 6/0/2 is currently active. |
| Line protocol on Interface Serial6/0/2, changed state to up | Indicates that the software processes that handle the line protocol consider the line usable for serial interface 6/0/2. |
| Serial6/0/2 address 2001:0DB8::248 add download succeeded | The IPv6 address 2001:0DB8::248 was downloaded successfully. |

Related Commands

| Command | Description |
|-----------------------------|---|
| debug ipv6 cef table | Displays debug messages for CEFv6 and dCEFv6 table modification events. |

debug ipv6 cef hash

To display debug messages for Cisco Express Forwarding CEF for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) load-sharing hash algorithm events, use the **debug ipv6 cef hash** command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 load-sharing hash algorithm events, use the **no** form of this command.

debug ipv6 cef hash

no debug ipv6 cef hash

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging for CEFv6 and dCEFv6 load-sharing hash algorithm events is not enabled.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.0(22)S | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **debug ipv6 cef hash** command is similar to the **debug ip cef hash** command, except that it is IPv6-specific.

Use this command when changing the load-sharing algorithm to display IPv6 hash table details.



Note

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the Release 12 *Cisco IOS Debug Command Reference*.

Related Commands

| Command | Description |
|------------------------------|---|
| debug ipv6 cef events | Displays debug messages for CEFv6 and dCEFv6 general events. |
| debug ipv6 cef table | Displays debug messages for CEFv6 and dCEFv6 table modification events. |

debug ipv6 cef receive

To display debug messages for Cisco Express Forwarding CEF for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) packets that are process-switched on the router, use the **debug ipv6 cef receive** command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 packets that are process-switched on the router, use the **no** form of this command.

debug ipv6 cef receive

no debug ipv6 cef receive

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging for CEFv6 and dCEFv6 packets that are process-switched on the router is not enabled.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.0(22)S | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **debug ipv6 cef receive** command is similar to the **debug ip cef receive** command, except that it is IPv6-specific.



Note

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the Release 12 *Cisco IOS Debug Command Reference*.

Examples

The following is sample output from the **debug ipv6 cef receive** command when another router in the network pings 2001:0DB8::2 which is a local address on this box:

```
Router# debug ipv6 cef receive
```

```
IPv6 CEF packet receives debugging is on
router#
*Aug 30 08:25:14.869: IPv6CEF-receive: Receive packet for 2001:0DB8::2
*Aug 30 08:25:14.897: IPv6CEF-receive: Receive packet for 2001:0DB8::2
*Aug 30 08:25:14.925: IPv6CEF-receive: Receive packet for 2001:0DB8::2
*Aug 30 08:25:14.953: IPv6CEF-receive: Receive packet for 2001:0DB8::2
*Aug 30 08:25:14.981: IPv6CEF-receive: Receive packet for 2001:0DB8::2
```

Table 10 describes the significant fields shown in the display.

Table 10 *debug ipv6 cef receive Field Descriptions*

| Field | Description |
|--|--|
| IPv6CEF-receive: Receive packet for 2001:0DB8::2 | CEF has received a packet addressed to the router. |

Related Commands

| Command | Description |
|------------------------------|---|
| debug ipv6 cef events | Displays debug messages for CEFv6 and dCEFv6 general events. |
| debug ipv6 cef table | Displays debug messages for CEFv6 and dCEFv6 table modification events. |

debug ipv6 cef table

To display debug messages for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) table modification events, use the **debug ipv6 cef table** command in privileged EXEC mode. To disable debug messages for CEFv6 and dCEFv6 table modification events, use the **no** form of this command.

debug ipv6 cef table [**background**]

no debug ipv6 cef table [**background**]

| | |
|---------------------------|--|
| Syntax Description | background (Optional) Sets CEFv6 and dCEFv6 table background updates. |
|---------------------------|--|

| | |
|-----------------|--|
| Defaults | Debugging for CEFv6 and dCEFv6 table modification events is not enabled. |
|-----------------|--|

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release | Modification |
|------------------------|----------------|---|
| | 12.0(22)S | This command was introduced. |
| | 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

| | |
|-------------------------|---|
| Usage Guidelines | The debug ipv6 cef table command is similar to the debug ip cef table command, except that it is IPv6-specific. |
| | This command is used to record CEFv6 and dCEFv6 table events related to the Forwarding Information Base (FIB) tables. Types of events include the following: <ul style="list-style-type: none"> • Routing updates that populate the FIB tables • Flushing of the FIB tables • Adding or removing of entries to the FIB tables • Table reloading process |



Note

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options in global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*.

| | |
|-----------------|--|
| Examples | The following is sample output from the debug ipv6 cef table command when a static route is added: Router# debug ipv6 cef table |
|-----------------|--|

IPv6 CEF table debugging is on

```
router(config)# ipv6 route 5555::/64 serial 2/0 3000::2
router(config)#
*Feb 24 08:46:09.187: IPv6CEF-Table: Event add, 5555::/64
*Feb 24 08:46:09.187: IPv6 CEF table: Created path_list 01184570
*Feb 24 08:46:09.187: IPv6 CEF table: Adding path 01181A80 to path_list 01184570 old path
count=0
*Feb 24 08:46:09.187: IPv6 CEF table: No matching list for path list 01184570
*Feb 24 08:46:09.187: IPv6 CEF table: Adding fib entry 0117EE80 to path_list 01184570 old
refcount=0
*Feb 24 08:46:09.187: IPv6 CEF table: Added path_list 01184570 to hash 50
*Feb 24 08:46:09.187: IPv6 CEF: Linking path 01181A80 to adjacency 01138E28
*Feb 24 08:46:09.187: IPv6 CEF table: Created 0 loadinfos for path_list 01184570
*Feb 24 08:46:09.187: IPv6CEF-Table: Validated 5555::/64
```

The following is sample output when the static route is removed:

```
router(config)# no ipv6 route 5555::/64 serial 2/0 3000::2
router(config)#
*Feb 24 08:46:43.871: IPv6CEF-Table: Event delete, 5555::/64
*Feb 24 08:46:43.871: IPv6CEF-Table: Invalidated 5555::/64
*Feb 24 08:46:43.871: IPv6CEF-Table: Deleted 5555::/64
*Feb 24 08:46:43.871: IPv6 CEF table: Removing fib entry 0117EE80 from path_list 01184570
old refcount=1
*Feb 24 08:46:43.871: IPv6 CEF table: Removed path_list 01184570 from hash 50
*Feb 24 08:46:43.871: IPv6 CEF table: Freeing path_list 01184570 refcount=0
*Feb 24 08:46:43.871: IPv6 CEF table: Freeing all 1 paths in path_list 01184570
*Feb 24 08:46:43.871: IPv6 CEF: deleting path 01181A80
```

| Related Commands | Command | Description |
|------------------|-----------------------|--|
| | debug ipv6 cef events | Displays debug messages for CEFv6 and dCEFv6 general events. |

debug ipv6 dhcp

To enable debugging for Dynamic Host Configuration Protocol (DHCP) for IPv6, use the **debug ipv6 dhcp** command in privileged EXEC mode. To disable debugging for DHCP for IPv6, use the **no** form of this command.

debug ipv6 dhcp [detail]

no debug ipv6 dhcp [detail]

| | | |
|--------------------|---|---|
| Syntax Description | detail (Optional) Displays detailed information about DHCP for IPv6 message decoding. | |
| Defaults | Debugging for the DHCP for IPv6 is disabled. | |
| Command Modes | Privileged EXEC | |
| Command History | Release | Modification |
| | 12.3(4)T | This command was introduced. |
| Usage Guidelines | The detail keyword used with the debug ipv6 dhcp command reports detailed DHCP for IPv6 message decoding. | |
| Examples | The following example enables debugging for the DHCP for IPv6: Router# debug ipv6 dhcp | |
| Related Commands | Command | Description |
| | debug ipv6 dhcp database | Enables debugging for the DHCP for IPv6 binding database agent. |

debug ipv6 dhcp database

To enable debugging for the Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent, use the **debug ipv6 dhcp database** command in privileged EXEC mode. To disable the display of debug messages for the DHCP for IPv6 binding database agent, use the **no** form of this command.

debug ipv6 dhcp database

no debug ipv6 dhcp database

Syntax Description

This command has no keywords or arguments.

Defaults

Debugging for the DHCP for IPv6 binding database agent is disabled.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|----------|------------------------------|
| 12.3(4)T | This command was introduced. |

Usage Guidelines

The debug ipv6 dhcp database command enables debugging for DHCP for IPv6 database processing.

Examples

The following example enables debugging for the DHCP for IPv6 binding database agent:

```
Router# debug ipv6 dhcp database
```

Related Commands

| Command | Description |
|------------------------|--------------------------------------|
| debug ipv6 dhcp | Enables debugging for DHCP for IPv6. |

debug ipv6 icmp

To display debug messages for IPv6 Internet Control Message Protocol (ICMP) transactions (excluding IPv6 ICMP neighbor discovery transactions), use the **debug ipv6 icmp** command in privileged EXEC mode. To disable debug messages for IPv6 ICMP transactions, use the **no** form of this command.

debug ipv6 icmp

no debug ipv6 icmp

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging for IPv6 ICMP is not enabled.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **debug ipv6 icmp** command is similar to the **debug ip icmp** command, except that it is IPv6-specific.



Note

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options within global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the Release 12, *Cisco IOS Debug Command Reference*.

This command helps you determine whether the router is sending or receiving IPv6 ICMP messages. Use it, for example, when you are troubleshooting an end-to-end connection problem.



Note

For more information about the fields in **debug ipv6 icmp** output, refer to RFC 2463, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)*.

Examples

The following example shows output for the **debug ipv6 icmp** command:

```
Router# debug ipv6 icmp
```

```
13:28:40:ICMPv6:Received ICMPv6 packet from 2000:0:0:3::2, type 136
```

```

13:28:45:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
13:28:50:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 136
13:28:55:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135

```

Table 11 describes significant fields shown in the first line of the display.

Table 11 *debug ipv6 icmp Field Descriptions*

| Field | Description |
|---------------------------------------|--|
| 13:28:40: | Indicates the time (hours:minutes:seconds) at which the ICMP neighbor discovery event occurred. |
| nwnd: (not shown in sample output) | Indicates time (weeks, days) since last reboot of the event occurring. For example, 1w4d: indicates the time (since the last reboot) of the event occurring was 1 week and 4 days ago. |
| ICMPv6: | Indication that this message describes an ICMP version 6 packet. |

Table 11 *debug ipv6 icmp Field Descriptions (continued)*

| Field | Description |
|--|---|
| Received ICMPv6 packet from 2001:0DB8:0:3::2 | IPv6 address from which the ICMP version 6 packet is received. |
| type 135 | <p>The number variable indicates one of the following IPv6 ICMP message types:</p> <ul style="list-style-type: none"> • 1—Destination unreachable. The router cannot forward a packet that was sent or received. • 2—Packet too big. The router attempts to send a packet that exceeds the maximum transmission unit (MTU) of a link between itself and the packet destination. • 3—Time exceeded. Either the hop limit in transit or the fragment reassembly time is exceeded. • 4—Parameter problem. The router attempts to send an IPv6 packet that contains invalid parameters. An example is a packet containing a next header type unsupported by the router that is forwarding the packet. • 128—Echo request. The router received an echo reply. • 129—Echo reply. The router sent an echo reply. • 133—Router solicitation messages. Hosts send these messages to prompt routers on the local link to send router advertisement messages. • 134—Router advertisement messages. Routers periodically send these messages to advertise their link-layer addresses, prefixes for the link, and other link specific information. These messages are also sent in response to router solicitation messages. • 135—Neighbor solicitation messages. Nodes send these messages to request the link-layer address of a station on the same link. • 136—Neighbor advertisement messages. Nodes send these messages, containing their link-local addresses, in response to neighbor solicitation messages. • 137—Redirect messages. Routers send these messages to hosts when a host attempts to use a less-than-optimal first hop address when forwarding packets. These messages contain a better first hop address that should be used instead. |

Following are examples of the IPv6 ICMP messages types that can be displayed by the **debug ipv6 icmp** command:

- ICMP echo request and ICMP echo reply messages. In the following example, an ICMP echo request is sent to address 2052::50 and an ICMP echo reply is received from address 2052::50.

```
1w4d:ICMPv6:Sending echo request to 2052::50
1w4d:ICMPv6:Received echo reply from 2052::50
```

- ICMP packet too big messages. In the following example, a router tried to forward a packet to destination address 2052::50 via the next hop address 2052::52. The size of the packet was greater than 1280 bytes, which is the MTU of destination address 2052::50. As a result, the router receives an ICMP packet too big message from the next hop address 2052::52.

```
1w4d:Received ICMP too big from 2052::52 about 2052::50, MTU=1300
```

- ICMP parameter problem messages. In the following example, an ICMP parameter problem message is received from address 2052::52.

```
1w4d:Received ICMP parameter problem from 2052::52
```

- ICMP time exceeded messages. In the following example, an ICMP time exceeded message is received from address 2052::52.

```
1w4d:Received ICMP time exceeded from 2052::52
```

- ICMP unreachable messages. In the following example, an ICMP unreachable message with code 1 is received from address 2052::52. Additionally, an ICMP unreachable message with code 1 is sent to address 2060::20 about address 2062::20.

```
1w4d:Received ICMP unreachable code 1 from 2052::52
```

```
1w4d:Sending ICMP unreachable code 1 to 2060::20 about 2062::20
```

Table 12 lists the codes for ICMP unreachable messages.

Table 12 *ICMP Unreachable Message—Code Descriptions*

| Code | Description |
|------|--|
| 0 | The router has no route to the packet destination. |
| 1 | Although the router has a route to the packet destination, communication is administratively prohibited. |
| 3 | The address is unreachable. |
| 4 | The port is unreachable. |

Related Commands

| Command | Description |
|----------------------|--|
| debug ipv6 nd | Displays debug messages for IPv6 ICMP neighbor discovery transactions. |

debug ipv6 mfib

To enable debugging output on the IPv6 Multicast Forwarding Information Base (MFIB), use the **debug ipv6 mfib** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mfib { **adjacency** | **signal** | **db** | **init** | **mrrib** | **pak** | **ps** } [*group-name* | *group-address*]

no debug ipv6 mfib { **adjacency** | **signal** | **db** | **init** | **mrrib** | **pak** | **ps** } [*group-name* | *group-address*]

Syntax Description

| | |
|--|---|
| adjacency | Adjacency management activity. |
| signal | MFIB data-driven signaling to routing protocols. |
| db | Route database management activity. |
| init | Initialization or de-initialization activity |
| mrrib | Communication with the MRIB. |
| pak | Packet forwarding activity. |
| ps | Process-level-only additional packet forwarding activity. |
| <i>group-name</i> <i>group-address</i> | (Optional) IPv6 address or name of the multicast group. |

Command Modes

Privileged EXEC

Syntax Description

| Release | Modification |
|-----------|---|
| 12.3(2)T | This command was introduced. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

You must use at least one keyword to enable debugging output for this command.

Examples

The following example enables debugging output for packet forwarding activity on the IPv6 MFIB for destination address ff04::10:

```
Router# debug ipv6 mfib pak FF04::10
```

debug ipv6 mld

To enable debugging on Multicast Listener Discovery (MLD) protocol activity, use the **debug ipv6 mld** command in privileged EXEC mode. To restore the default value, use the **no** form of this command.

```
debug ipv6 mld [group-name | group-address | interface-type]
```

```
no debug ipv6 mld [group-name | group-address | interface-type]
```

In Cisco IOS Release 12.0(26)S, the syntax is as follows:

```
debug ipv6 mld [group group-name | group-address | interface interface-type]
```

```
no debug ipv6 mld [group group-name | group-address | interface interface-type]
```

Syntax Description

| | |
|--|--|
| <i>group-name</i> <i>group-address</i> or group <i>group-name</i> <i>group-address</i> | (Optional) IPv6 address or name of the multicast group. |
| <i>interface-type</i> or interface <i>interface-type</i> | (Optional) Interface type. For more information, use the question mark (?) online help function. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.3(2)T | This command was introduced. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

This command helps discover whether the MLD protocol activities are working correctly. In general, if MLD is not working, the router process never discovers that there is a host on the network that is configured to receive multicast packets.

The messages displayed by the **debug ipv6 mld** command show query and report activity received from other routers and hosts. Use this command in conjunction with **debug ipv6 pim** to display additional multicast activity, to learn more information about the multicast routing process, or to learn why packets are forwarded out of particular interfaces.

Examples

The following example enables debugging on MLD protocol activity:

```
Router# debug ipv6 mld
```

Related Commands

| Command | Description |
|-----------------------|---|
| debug ipv6 pim | Enables debugging on PIM protocol activity. |

debug ipv6 mrib client

To enable debugging on Multicast Routing Information Base (MRIB) client management activity, use the **debug ipv6 mrib client** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mrib client

no debug ipv6 mrib client

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

The **debug ipv6 mrib client** command is used to display the activity in the MRIB associated with clients such as Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD). If you are having difficulty with your client connections, use this command to display new clients being added and deleted.

The **debug ipv6 mrib client** command also displays information on when a new client is added to or deleted from the MRIB, when a client connection is established or torn down, when a client binds to a particular MRIB table, and when a client is informed that there are updates to be read.

Examples

The following example enables debugging on MRIB client management activity:

```
Router# debug ipv6 mrib client
```

| Related Commands | Command | Description |
|------------------|------------------------------|---|
| | debug ipv6 mrib route | Displays MRIB routing entry-related activity. |

debug ipv6 mrib io

To enable debugging on Multicast Routing Information Base (MRIB) I/O events, use the **debug ipv6 mrib io** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mrib io

no debug ipv6 mrib io

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.3(2)T | This command was introduced. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

Use the **debug ipv6 mrib io** command to display information on when clients open and close MRIB I/O connections, when MRIB entry and interface updates are received and processed from clients, and when MRIB entry and interface updates are sent to clients.

Examples

The following example enables debugging on MRIB I/O events:

```
Router# debug ipv6 mrib io
```

debug ipv6 mrib proxy

To enable debugging on multicast routing information base (MRIB) proxy activity between the route processor and line cards on distributed router platforms, use the **debug ipv6 mrib proxy** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mrib proxy

no debug ipv6 mrib proxy

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|--|
| | 12.0(26)S | This command was introduced. |
| | 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines Use the **debug ipv6 mrib proxy** command to display information on connections that are being opened and closed and on MRIB transaction messages that are being passed between the route processor and line cards.

Examples The following example enables debugging on MRIB proxy events:

Router# **debug ipv6 mrib proxy**

debug ipv6 mrib route

To display information about Multicast Routing Information Base (MRIB) routing entry-related activity, use the **debug ipv6 mrib route** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 mrib route [*group-name* | *group-address*]

no debug ipv6 mrib route

Syntax Description

| | |
|---|--|
| <i>group-name</i> <i>group-address</i> | (Optional)IPv6 address or name of the multicast group. |
|---|--|

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.3(2)T | This command was introduced. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

This command displays update information related to the route database made by MRIB clients, which is then redistributed to the clients.

Use this command to monitor MRIB route activity when discontinuity is found between the MRIB and the client database or between the individual client databases.

Examples

The following example enables the display of information about MRIB routing entry-related activity:

```
Router# debug ipv6 mrib route
```

Related Commands

| Command | Description |
|------------------------------|---|
| show ipv6 mrib client | Displays information about the MRIB client management activity. |

debug ipv6 mrib table

To enable debugging on Multicast Routing Information Base (MRIB) table management activity, use the **debug ipv6 mrib table** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ipv6 mrib table
no debug ipv6 mrib table
```

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines Use the **debug ipv6 mrib table** command to display information on new MRIB tables being added and deleted.

Examples The following example enables debugging on MRIB table management activity:

```
Router# debug ipv6 mrib table
```

debug ipv6 nat

To display debugging messages for Network Address Translation - Protocol Translation (NAT-PT) translation events, use the **debug ipv6 nat** command in privileged EXEC mode. To disable debugging messages for NAT-PT translation events, use the **no** form of this command.

debug ipv6 nat [**detailed** | **port**]

no debug ipv6 nat [**detailed** | **port**]

Syntax Description

| | |
|-----------------|---|
| detailed | (Optional) Displays detailed information about NAT-PT translation events. |
| port | (Optional) Displays port allocation events. |

Defaults

Debugging for NAT-PT translation events is not enabled.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|--|
| 12.2(13)T | This command was introduced. |
| 12.3(2)T | The port keyword was added to support Port Address Translation (PAT), or overload, multiplexing multiple IPv6 addresses to a single IPv4 address or to an IPv4 address pool. |

Usage Guidelines

The **debug ipv6 nat** command can be used to troubleshoot NAT-PT translation issues. If no keywords are specified, debugging messages for all NAT-PT protocol translation events are displayed.



Note

By default, the network server sends the output from **debug** commands and system error messages to the console. To redirect debugging output, use the logging command options within global configuration mode. Destinations are the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on **debug** commands and redirecting debugging output, refer to the Release 12.2 *Cisco IOS Debug Command Reference*.



Caution

Because the **debug ipv6 nat** command generates a substantial amount of output, use it only when traffic on the IPv6 network is low, so other activity on the system is not adversely affected.

Examples

The following example shows output for the **debug ipv6 nat** command:

```
Router# debug ipv6 nat
```

```
00:06:06: IPv6 NAT: icmp src (3002::8) -> (192.168.124.8), dst (2001::2) ->
(192.168.123.2)
00:06:06: IPv6 NAT: icmp src (192.168.123.2) -> (2001::2), dst (192.168.124.8) ->
(3002::8)
00:06:06: IPv6 NAT: icmp src (3002::8) -> (192.168.124.8), dst (2001::2) ->
(192.168.123.2)
00:06:06: IPv6 NAT: icmp src (192.168.123.2) -> (2001::2), dst (192.168.124.8) ->
(3002::8)
00:06:06: IPv6 NAT: tcp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: tcp src (192.168.123.2) -> (2001::2), dst (192.168.124.8) -> (3002::8)
00:06:06: IPv6 NAT: tcp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: tcp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: tcp src (3002::8) -> (192.168.124.8), dst (2001::2) -> (192.168.123.2)
00:06:06: IPv6 NAT: tcp src (192.168.123.2) -> (2001::2), dst (192.168.124.8) -> (3002::8)
```

Table 13 describes the significant fields shown in the display.

Table 13 *debug ipv6 nat Field Descriptions*

| Field | Description |
|----------------------------------|---|
| IPv6 NAT: | Indicates that this is a NAT-PT packet. |
| icmp | Protocol of the packet being translated. |
| src (3000::8) -> (192.168.124.8) | The source IPv6 address and the NAT-PT mapped IPv4 address. Note If mapping IPv4 hosts to IPv6 hosts the first address would be an IPv4 address, and the second address an IPv6 address. |
| dst (2001::2) -> (192.168.123.2) | The destination IPv6 address and the NAT-PT mapped IPv4 address. Note If mapping IPv4 hosts to IPv6 hosts the first address would be an IPv4 address, and the second address an IPv6 address. |

The following example shows output for the **debug ipv6 nat** command with the **detailed** keyword:

```
Router# debug ipv6 nat detailed
```

```
00:14:12: IPv6 NAT: address allocated 192.168.124.8
00:14:16: IPv6 NAT: deleted a NAT entry after timeout
```

debug ipv6 nd

To display debug messages for IPv6 Internet Control Message Protocol (ICMP) neighbor discovery transactions, use the **debug ipv6 nd** command in privileged EXEC mode. To disable debug messages for IPv6 ICMP neighbor discovery transactions, use the **no** form of this command.

debug ipv6 nd

no debug ipv6 nd

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging for IPv6 ICMP neighbor discovery is not enabled.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------|---|
| 12.2(2)T | This command was introduced. |
| 12.2(4)T | The DAD: <nnnn::nn> is unique, DAD: duplicate link-local <nnnn::nn> on <interface type>, interface stalled, and Received NA for <nnnn::nn> on <interface type> from <nnnn::nn> fields were added to the command output. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

This command can help determine whether the router is sending or receiving IPv6 ICMP neighbor discovery messages.



Note

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options within global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*.

Examples

The following example shows output for the **debug ipv6 nd** command:

```
Router# debug ipv6 nd
```

```
13:22:40:ICMPv6-ND:STALE -> DELAY:2000:0:0:3::2
13:22:45:ICMPv6-ND:DELAY -> PROBE:2000:0:0:3::2
13:22:45:ICMPv6-ND:Sending NS for 2000:0:0:3::2 on FastEthernet0/0
13:22:45:ICMPv6-ND:Received NA for 2000:0:0:3::2 on FastEthernet0/0 from 2000:0:0:3::2
```

```

13:22:45:ICMPv6-ND:PROBE -> REACH:2000:0:0:3::2
13:22:45:ICMPv6-ND:Received NS for 2000:0:0:3::1 on FastEthernet0/0 from
FE80::203:A0FF:FED6:1400
13:22:45:ICMPv6-ND:Sending NA for 2000:0:0:3::1 on FastEthernet0/0

13:23:15: ICMPv6-ND: Sending NS for FE80::1 on Ethernet0/1
13:23:16: ICMPv6-ND: DAD: FE80::1 is unique.
13:23:16: ICMPv6-ND: Sending NS for 2000::2 on Ethernet0/1
13:23:16: ICMPv6-ND: Sending NS for 3000::3 on Ethernet0/1
13:23:16: ICMPv6-ND: Sending NA for FE80::1 on Ethernet0/1
13:23:17: ICMPv6-ND: DAD: 2000::2 is unique.
13:23:53: ICMPv6-ND: Sending NA for 2000::2 on Ethernet0/1
13:23:53: ICMPv6-ND: DAD: 3000::3 is unique.
13:23:53: ICMPv6-ND: Sending NA for 3000::3 on Ethernet0/1
3d19h: ICMPv6-ND: Sending NS for FE80::2 on Ethernet0/2
3d19h: ICMPv6-ND: Received NA for FE80::2 on Ethernet0/2 from FE80::2
3d19h: ICMPv6-ND: DAD: duplicate link-local FE80::2 on Ethernet0/2,interface stalled
3d19h: %IPV6-4-DUPLICATE: Duplicate address FE80::2 on Ethernet0/2
3d19h: ICMPv6-ND: Sending NS for 3000::4 on Ethernet0/3
3d19h: ICMPv6-ND: Received NA for 3000::4 on Ethernet0/3 from 3000::4
3d19h: %IPV6-4-DUPLICATE: Duplicate address 3000::4 on Ethernet0/3

```

Table 14 describes the significant fields shown in the display.

Table 14 *debug ipv6 nd Field Descriptions*

| Field | Description |
|--------------------|--|
| 13:22:40: | Indicates the time (hours:minutes:seconds) at which the ICMP neighbor discovery event occurred. |
| ICMPv6-ND | Indicates that a state change is occurring for an entry in the IPv6 neighbors cache. |
| STALE | Stale state. This state of an neighbor discovery cache entry used to be “reachable,” but is now is “stale” due to the entry not being used. In order to use this address, the router must go through the neighbor discovery process in order to confirm reachability. |
| DELAY | Delayed state. Reachability for this ND cache entry is currently being reconfirmed. While in the delay state, upper-layer protocols may inform IPv6 that they have confirmed reachability to the entry. Therefore, there is no need to send a neighbor solicitation for the entry. |
| PROBE | Probe state. While in the probe state, if no confirmation is received from the upper-layer protocols about the reachability of the entry, a neighbor solicitation message is sent. The entry remains in the “probe” state until a neighbor advertisement message is received in response to the neighbor solicitation message. |
| Sending NS for... | Sending a neighbor solicitation message. In the example output, a neighbor solicitation message is sent on Fast Ethernet interface 0/0 to determine the link-layer address of 2000:0:0:3::2 on Fast Ethernet interface 0/0. |
| Received NA for... | Received a neighbor advertisement message. In the example output, a neighbor advertisement message is received from the address 2000:0:0:3::2 (the second address) that includes the link-layer address of 2000:0:0:3::2 (first address) from Ethernet interface 0/0. |

Table 14 *debug ipv6 nd Field Descriptions (continued)*

| Field | Description |
|---|---|
| REACH | Reachable state. An ND cache entry in this state is considered reachable, and the corresponding link-layer address can be used without needing to perform neighbor discovery on the address. |
| Received NS for... | Received neighbor solicitations. In the example output, the address FE80::203:A0FF:FED6:1400 (on Fast Ethernet interface 0/0) is trying to determine the link-local address of 2000:0:0:3::1. |
| Sending NA for... | Sending for neighbor advertisements. In the example output, a neighbor advertisement containing the link-layer address of 2000:0:0:3::1 (an address assigned to the Fast Ethernet interface 0/0 address) was sent. |
| DAD: FE80::1 is unique. | Duplicate address detection processing was performed on the unicast IPv6 address (a neighbor solicitation message was not received in response to a neighbor advertisement message that contained the unicast IPv6 address) and the address is unique. |
| 3d19h: | Indicates time (days, hours) since the last reboot of the event occurring; 3d19h: indicates the time (since the last reboot) of the event occurring was 3 days and 19 hours ago. |
| DAD: duplicate link-local FE80::2 on Ethernet0/2, interface stalled | Duplicate address detection processing was performed on the link-local IPv6 address (the link-local address FE80::2 is used in the example). A neighbor advertisement message was received in response to a neighbor solicitation message that contained the link-local IPv6 address. The address is not unique, and the processing of IPv6 packets is disabled on the interface. |
| %IPv6-4-DUPLICATE: Duplicate address... | System error message indicating the duplicate address. |
| Received NA for 3000::4 on Ethernet0/3 from 3000::4 | Duplicate address detection processing was performed on the global IPv6 address (the global address 3000::4 is used in the example). A neighbor advertisement message was received in response to a neighbor solicitation message that contained the global IPv6 address. The address is not unique and is not used. |

Related Commands

| Command | Description |
|----------------------------|---|
| debug ipv6 icmp | Displays debug messages for IPv6 ICMP transactions. |
| show ipv6 neighbors | Displays IPv6 neighbor discovery cache information. |

debug ipv6 ospf

To display debugging information for Open Shortest Path First (OSPF) for IPv6, use the **debug ipv6 ospf** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ipv6 ospf [adj | authentication | database-timer | flood | hello | lsa-generation |
retransmission]

no debug ipv6 ospf [adj | authentication | database-timer | flood | hello | lsa-generation |
retransmission]
```

| | | |
|--------------------|----------------|--|
| Syntax Description | adj | (Optional) Displays adjacency information. |
| | database-timer | (Optional) Displays database-timer information. |
| | authentication | (Optional) Displays the interaction between OSPF and IPsec in IPv6 networks, including creation and removal of policy definitions. |
| | flood | (Optional) Displays flooding information. |
| | hello | (Optional) Displays hello packet information. |
| | lsa-generation | (Optional) Displays link-state advertisement (LSA) generation information for all LSA types. |
| | retransmission | (Optional) Displays retransmission information. |

Defaults Debugging of IPsec OSPF is not enabled.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.3(4)T | The authentication keyword was added to support OSPF authentication for IPv6 IPsec. |

Usage Guidelines Consult Cisco technical support before using this command.

Examples The following example displays adjacency information for OSPF for IPv6:
Router# debug ipv6 ospf adj

debug ipv6 ospf events

To display information on OSPF-related events, such as designated router selection and shortest path first (SPF) calculation, use the **debug ipv6 ospf events** command in privileged EXEC command. To disable debugging output, use the **no** form of this command.

debug ipv6 ospf events

no debug ipv6 ospf events

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines Consult Cisco technical support before using this command.

Examples The following example displays information on OSPF-related events:

```
Router# debug ipv6 ospf events
```

debug ipv6 ospf lsdb

To display database modifications for OSPF for IPv6, use the **debug ipv6 ospf lsdb** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 ospf lsdb

no debug ipv6 ospf lsdb

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines Consult Cisco technical support before using this command.

Examples The following example displays database modification information for OSPF for IPv6:

```
Router# debug ipv6 ospf lsdb
```

debug ipv6 ospf packet

To display information about each OSPF for IPv6 packet received, use the **debug ipv6 ospf packet** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 ospf packet

no debug ipv6 ospf packet

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines Consult Cisco technical support before using this command.

Examples The following example displays information about each OSPF for IPv6 packet received:

```
Router# debug ipv6 ospf packet
```

debug ipv6 ospf spf statistic

To display statistical information while running the shortest path first (SPF) algorithm, use the **debug ipv6 ospf spf statistic** command in privileged EXEC mode. To disable the debugging output, use the **no** form of this command.

debug ipv6 ospf spf statistic

no debug ipv6 ospf spf statistic

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines The **debug ipv6 ospf spf statistic** command displays the SPF calculation times in milliseconds, the node count, and a time stamp. Consult Cisco technical support before using this command.

Examples The following example displays statistical information while running the SPF algorithm:

```
Router# debug ipv6 ospf spf statistics
```

| Related Commands | Command | Description |
|------------------|-------------------------------|---|
| | debug ipv6 ospf | Displays debugging information for the OSPFv3 for IPv6 feature. |
| | debug ipv6 ospf events | Displays information on OSPFv3-related events. |
| | debug ipv6 ospf packet | Displays information about each OSPFv3 packet received. |

debug ipv6 packet

To display debug messages for IPv6 packets, use the **debug ipv6 packet** command in privileged EXEC mode. To disable debug messages for IPv6 packets, use the **no** form of this command.

debug ipv6 packet [**access-list** *access-list-name*] [**detail**]

no debug ipv6 packet [**access-list** *access-list-name*] [**detail**]

| | | |
|---------------------------|-------------------------|--|
| Syntax Description | access-list | (Optional) Specifies an IPv6 access list. The access list name cannot contain a space or quotation mark, or begin with a numeric |
| | <i>access-list-name</i> | |
| | detail | (Optional) Displays detailed information about a specified IPv6 access list. |

Defaults Debugging for IPv6 packets is not enabled.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|------------------------|----------------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.0(23)S, 12.2(13)T | The access-list and detail keywords, and the <i>access-list-name</i> argument, were added. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines The **debug ipv6 packet** command is similar to the **debug ip packet** command, except that it is IPv6-specific.



Note

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options within global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*.

IPv6 debugging information includes packets received, generated, and forwarded. Fast-switched packets do not generate messages. When an IPv6 access list is specified by using the **access-list** keyword and *access-list-name* argument, only packets matching the access list permit entries are displayed.



Caution

Because the **debug ipv6 packet** command generates a substantial amount of output, use it only when traffic on the IPv6 network is low, so other activity on the system is not adversely affected.

Examples

The following example shows output for the **debug ipv6 packet** command:

```
Router# debug ipv6 packet
```

```
13:25:40:IPv6:source 2000:0:0:3::1 (local)
13:25:40:      dest 2000:0:0:3::2 (FastEthernet0/0)
13:25:40:      traffic class 96, flow 0x0, len 143+195, prot 6, hops 64, originating
13:25:40:IPv6:Sending on FastEthernet0/0
13:25:40:IPv6:source 2000:0:0:3::2 (FastEthernet0/0)
13:25:40:      dest 2000:0:0:3::1
13:25:40:      traffic class 96, flow 0x0, len 60+14, prot 6, hops 64, forward to ulp
13:25:45:IPv6:source FE80::203:E4FF:FE12:CC1D (local)
13:25:45:      dest FF02::9 (Ethernet1/1)
13:25:45:      traffic class 112, flow 0x0, len 72+1428, prot 17, hops 255, originating
13:25:45:IPv6:Sending on Ethernet1/1
13:25:45:IPv6:source FE80::203:E4FF:FE12:CC00 (local)
13:25:45:      dest 2000:0:0:3::2 (FastEthernet0/0)
13:25:45:      traffic class 112, flow 0x0, len 72+8, prot 58, hops 255, originating
13:25:45:IPv6:Sending on FastEthernet0/0
13:25:45:IPv6:source 2000:0:0:3::2 (FastEthernet0/0)
13:25:45:      dest FE80::203:E4FF:FE12:CC00
13:25:45:      traffic class 112, flow 0x0, len 64+14, prot 58, hops 255, forward to ulp
13:25:45:IPv6:source FE80::203:A0FF:FED6:1400 (FastEthernet0/0)
13:25:45:      dest 2000:0:0:3::1
13:25:45:      traffic class 112, flow 0x0, len 72+14, prot 58, hops 255, forward to ulp
```

Table 15 describes the significant fields shown in the display.

Table 15 *debug ipv6 packet Field Descriptions*

| Field | Description |
|---|--|
| IPv6: | Indicates that this is an IPv6 packet. |
| source 2000:0:0:3::1 (local) | The source address in the IPv6 header of the packet. |
| dest 2000:0:0:3::2 (FastEthernet0/0) | The destination address in the IPv6 header of the packet. |
| traffic class 96 | The contents of the traffic class field in the IPv6 header. |
| flow 0x0 | The contents of the flow field of the IPv6 header. The flow field is used to label sequences of packets for which special handling is necessary by IPv6 routers. |
| len 143+195 | The length field of the IPv6 packet. The length is expressed as two numbers with a plus (+) character between the numbers. The second number is the length of the IPv6 portion (payload length plus IPv6 header length). The first number is the entire datagram size minus the second number. |
| prot 6 | The protocol field in the IPv6 header. Describes the next layer protocol that is carried by the IPv6 packet. In the example, the protocol 58 signifies that the next layer protocol is ICMPv6. |
| hops 64 | The hops field in the IPv6 packet. This field is similar in function to the IPv4 time-to-live field. |
| originating | The presence of this field indicates that the packet shown was originated by the router. |

Table 15 *debug ipv6 packet Field Descriptions (continued)*

| Field | Description |
|----------------------------|---|
| Sending on FastEthernet0/0 | Specifies the interface on which the packet was sent. |
| forward to ulp | Indicates that the packet was received by the router at the destination address and was forwarded to an upper-layer address (ulp) for processing. |

debug ipv6 pim

To enable debugging on Protocol Independent Multicast (PIM) protocol activity, use the **debug ipv6 pim** command in privileged EXEC mode. To restore the default value, use the **no** form of this command.

debug ipv6 pim [*group-name* | *group-address* | *interface-type* | **neighbor**]

no debug ipv6 pim [*group-name* | *group-address* | *interface-type* | **neighbor**]

Syntax Description

| | |
|--|--|
| <i>group-name</i> <i>group-address</i> | (Optional) IPv6 address or name of the multicast group. |
| <i>interface-type</i> | (Optional) Interface type. For more information, use the question mark (?) online help function. |
| neighbor | (Optional) Debug statistics related to hello message processing and neighbor cache management. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.3(2)T | This command was introduced. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

This command helps discover whether the PIM protocol activities are working correctly.

The messages displayed by the **debug ipv6 pim** command show all PIM protocol messages, such as joins and prunes, received from or sent to other routers. Use this command in conjunction with **debug ipv6 mld** to display additional multicast activity, to learn more information about the multicast routing process, or to learn why packets are forwarded out of particular interfaces.

Examples

The following example enables debugging on PIM activity:

```
Router# debug ipv6 pim
```

Related Commands

| Command | Description |
|-----------------------|---|
| debug ipv6 mld | Enables debugging on MLD protocol activity. |

debug ipv6 pool

To enable debugging on IPv6 prefix pools, use the `debug ipv6 pool` command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug ipv6 pool

no debug ipv6 pool

| | |
|---------------------------|--|
| Syntax Description | This command has no keywords or arguments. |
|---------------------------|--|

| | |
|-----------------|-------------------------|
| Defaults | No debugging is active. |
|-----------------|-------------------------|

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release | Modification |
|------------------------|-----------|------------------------------|
| | 12.2(13)T | This command was introduced. |

| | |
|-----------------|--|
| Examples | The following example enables debugging for IPv6 prefix pools: |
|-----------------|--|

```
Router# debug ipv6 pool
```

```
2w4d: IPv6 Pool: Deleting route/prefix 2001:0DB8::/29 to Virtual-Access1 for cisco
2w4d: IPv6 Pool: Returning cached entry 2001:0DB8::/29 for cisco on Virtual-Access1 to
pool1
2w4d: IPv6 Pool: Installed route/prefix 2001:0DB8::/29 to Virtual-Access1 for cisco
```

| Related Commands | Command | Description |
|-------------------------|-----------------------------|--|
| | ipv6 local pool | Configures a local IPv6 prefix pool. |
| | show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |
| | show ipv6 local pool | Displays information about defined IPv6 prefix pools. |

debug ipv6 rip

To display debug messages for IPv6 Routing Information Protocol (RIP) routing transactions, use the **debug ipv6 rip** command in privileged EXEC mode. To disable debug messages for IPv6 RIP routing transactions, use the **no** form of this command.

debug ipv6 rip [*interface-type interface-number*]

no debug ipv6 rip [*interface-type interface-number*]

Syntax Description

| | |
|-------------------------|--|
| <i>interface-type</i> | (Optional) The interface type about which to display debug messages. |
| <i>interface-number</i> | (Optional) The interface number about which to display debug messages. |

Defaults

IPv6 RIP debugging is not enabled.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **debug ipv6 rip** command is similar to the **debug ip rip** command, except that it is IPv6-specific.



Note

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options within global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*.



Caution

Using this command without arguments enables IPv6 RIP debugging for RIP packets that are sent and received on all router interfaces. Using this command with arguments enables IPv6 RIP debugging for RIP packets that are sent and received only on the specified interface.

Using this command on busy networks seriously degrades the performance of the router.

Examples

The following example shows output for the **debug ipv6 rip** command:

```
Router# debug ipv6 rip
```

```

13:09:10:RIPng:Sending multicast update on Ethernet1/1 for as1_rip
13:09:10:      src=FE80::203:E4FF:FE12:CC1D
13:09:10:      dst=FF02::9 (Ethernet1/1)
13:09:10:      sport=521, dport=521, length=32
13:09:10:      command=2, version=1, mbz=0, #rte=1
13:09:10:      tag=0, metric=1, prefix=::/0
13:09:28:RIPng:response received from FE80::202:FDFE:FE77:1E42 on Ethernet1/1 for as1_rip
13:09:28:      src=FE80::202:FDFE:FE77:1E42 (Ethernet1/1)
13:09:28:      dst=FF02::9
13:09:28:      sport=521, dport=521, length=32
13:09:28:      command=2, version=1, mbz=0, #rte=1
13:09:28:      tag=0, metric=1, prefix=2000:0:0:1:1::/80

```

The example shows two RIP packets; both are updates, known as “responses” in RIP terminology and indicated by a “command” value of 2. The first is an update sent by this router, and the second is an update received by this router. Multicast update packets are sent to all neighboring IPv6 RIP routers (all routers that are on the same links as the router sending the update, and that have IPv6 RIP enabled). An IPv6 RIP router advertises the contents of its routing table to its neighbors by periodically sending update packets over those interfaces on which IPv6 RIP is configured. An IPv6 router may also send “triggered” updates immediately following a routing table change. In this case the updates only includes the changes to the routing table. An IPv6 RIP router may solicit the contents of the routing table of a neighboring router by sending a Request (command=1) message to the router. The router will respond by sending an update (Response, command=2) containing its routing table. In the example, the received response packet could be a periodic update from the address FE80::202:FDFE:FE77:1E42 or a response to a RIP request message that was previously sent by the local router.

Table 16 describes the significant fields shown in the display.

Table 16 *debug ipv6 rip Field Descriptions*

| Field | Description |
|--------------|--|
| as1_rip | The name of the RIP process that is sending or receiving the update. |
| src | The address from which the update was originated. |
| dst | The destination address for the update. |
| sport, dport | The source and destination ports for the update. (IPv6 RIP uses port 521, as shown in the display.) |
| command | The command field within the RIP packet. A value of 2 indicates that the RIP packet is a response (update); a value of 1 indicates that the RIP packet is a request. |
| version | The version of IPv6 RIP being used. The current version is 1. |
| mbz | There must be a 0 (mbz) field within the RIP packet. |
| #rte | Indicates the number of routing table entries (RTEs) the RIP packet contains. |
| tag | <p>The tag, metric, and prefix fields are specific to each RTE contained in the update.</p> <p>The tag field is intended to allow for the flagging of IPv6 RIP “internal” and “external” routes.</p> <p>The metric field is the distance metric from the router (sending this update) to the prefix.</p> <p>The prefix field is the IPv6 prefix of the destination being advertised.</p> |
| metric | |
| prefix | |
| | |

Related Commands

| Command | Description |
|--------------------|---|
| debug ipv6 routing | Displays debug messages for IPv6 routing table updates and route cache updates. |

debug ipv6 routing

To display debug messages for IPv6 routing table updates and route cache updates, use the **debug ipv6 routing** command in privileged EXEC mode. To disable debug messages for IPv6 routing table updates and route cache updates, use the **no** form of this command.

debug ipv6 routing

no debug ipv6 routing

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging for IPv6 routing table updates and route cache updates is not enabled.

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **debug ipv6 routing** command is similar to the **debug ip routing** command, except that it is IPv6-specific.



Note

By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options within global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*.

Examples

The following example shows output for the **debug ipv6 routing** command:

```
Router# debug ipv6 routing

13:18:43:IPv6RT0:Add 2000:0:0:1:1::/80 to table
13:18:43:IPv6RT0:Better next-hop for 2000:0:0:1:1::/80, [120/2]
13:19:09:IPv6RT0:Add 2000:0:0:2::/64 to table
13:19:09:IPv6RT0:Better next-hop for 2000:0:0:2::/64, [20/1]
13:19:09:IPv6RT0:Add 2000:0:0:2:1::/80 to table
13:19:09:IPv6RT0:Better next-hop for 2000:0:0:2:1::/80, [20/1]
13:19:09:IPv6RT0:Add 2000:0:0:4::/64 to table
13:19:09:IPv6RT0:Better next-hop for 2000:0:0:4::/64, [20/1]
13:19:37:IPv6RT0:Add 2000:0:0:6::/64 to table
```

```
13:19:37:IPv6RT0:Better next-hop for 2000:0:0:6::/64, [20/2]
```

The **debug ipv6 routing** command displays messages whenever the routing table changes. For example, the following message indicates that a route to the prefix 2000:0:0:1:1::/80 was added to the routing table at the time specified in the message.

```
13:18:43:IPv6RT0:Add 2000:0:0:1:1::/80 to table
```

The following message indicates that the prefix 2000:0:0:2::/64 was already in the routing table; however, a received advertisement provided a lower cost path to the prefix. Therefore, the routing table was updated with the lower cost path. (The [20/1] in the example is the administrative distance [20] and metric [1] of the better path.)

```
13:19:09:IPv6RT0:Better next-hop for 2000:0:0:2::/64, [20/1]
```

Related Commands

| Command | Description |
|-----------------------|--|
| debug ipv6 rip | Displays debug messages for IPv6 RIP routing transactions. |

debug isis spf-events

To display a log of significant events during an IS-IS shortest-path first (SPF) computation, use the **debug isis spf-events** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug isis spf-events

no debug isis spf-events

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 12.0 | This command was introduced. |
| | 12.2(15)T | Support for IPv6 was added. |
| | 12.2(18)S | Support for IPv6 was added. |
| | 12.0(26)S | Support for IPv6 was added. |

Usage Guidelines This command displays information about significant events that occur during SPF-related processing.

Examples The following example displays significant events during an IS-IS SPF computation:

```
Router# debug isis spf-events

ISIS-Spf: Compute L2 IPv6 SPT
ISIS-Spf: Move 0000.0000.1111.00-00 to PATHS, metric 0
ISIS-Spf: Add 0000.0000.2222.01-00 to TENT, metric 10
ISIS-Spf: Move 0000.0000.2222.01-00 to PATHS, metric 10
ISIS-Spf: considering adj to 0000.0000.2222 (Ethernet3/1) metric 10, level 2, circuit 3,
adj 3
ISIS-Spf: (accepted)
ISIS-Spf: Add 0000.0000.2222.00-00 to TENT, metric 10
ISIS-Spf: Next hop 0000.0000.2222 (Ethernet3/1)
ISIS-Spf: Move 0000.0000.2222.00-00 to PATHS, metric 10
ISIS-Spf: Add 0000.0000.2222.02-00 to TENT, metric 20
ISIS-Spf: Next hop 0000.0000.2222 (Ethernet3/1)
ISIS-Spf: Move 0000.0000.2222.02-00 to PATHS, metric 20
ISIS-Spf: Add 0000.0000.3333.00-00 to TENT, metric 20
ISIS-Spf: Next hop 0000.0000.2222 (Ethernet3/1)
ISIS-Spf: Move 0000.0000.3333.00-00 to PATHS, metric 20
```

default-information originate (IPv6 IS-IS)

To inject an IPv6 default route into an Intermediate System-to-Intermediate System (IS-IS) IPv6 routing domain, use the **default-information originate** command in address family configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**route-map** *map-name*]

no default-information originate [**route-map** *map-name*]

Syntax Description

| | |
|----------------------------------|--|
| route-map <i>map-name</i> | (Optional) Route map should be used to advertise the default route conditionally. The <i>map-name</i> argument identifies a configured route map. |
|----------------------------------|--|

Defaults

Disabled

Command Modes

Address family configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(8)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **default-information originate** (IPv6 IS-IS) command is similar to the **default-information originate** (IS-IS) command, except that it is IPv6-specific.

If a router configured with this command has an IPv6 route to ::/0 in the routing table, IS-IS will originate an advertisement for ::/0 in its link-state packets (LSPs).

Without a route map, the default is advertised only in Level 2 LSPs. For Level 1 routing, there is another mechanism to find the default route, which is for the router to look for the closest Level 1 or Level 2 router. The closest Level 1 or Level 2 router can be found by looking at the attached bit (ATT) in Level 1 LSPs.

A route map can be used for two purposes:

- Make the router generate default in its Level 1 LSPs.
- Advertise ::/0 conditionally.

With a **match ipv6 address** *standard-access-list* command, you can specify one or more IPv6 routes that must exist before the router will advertise ::/0.

Examples

The following example shows the IPv6 default route (::/0) being advertised with all other routes in router updates:

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6
Router(config-router-af)# default-information originate
```

Related Commands

| Command | Description |
|------------------------------------|---|
| address-family ipv6 (IS-IS) | Specifies the IPv6 address family and places the router in address family configuration mode. |
| match ipv6 address | Distributes IPv6 routes that have a prefix permitted by a prefix list. |
| show isis database | Displays the IS-IS link-state database. |

deny (IPv6)

To set deny conditions for an IPv6 access list, use the **deny** command in IPv6 access list configuration mode. To remove the deny conditions, use the **no** form of this command.

```
deny {protocol} {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [dscp value] [flow-label value] [fragments] [log] [log-input]
[routing] [sequence value] [time-range name] [undetermined-transport]
```

```
no deny {protocol} {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [dscp value] [flow-label value] [fragments] [log] [log-input]
[routing] [sequence value] [time-range name] [undetermined-transport]
```

Internet Control Message Protocol

```
deny icmp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [icmp-type [icmp-code] | icmp-message] [dscp value] [flow-label
value] [fragments] [log] [log-input] [routing] [sequence value] [time-range name]
```

Transmission Control Protocol

```
deny tcp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [ack] [dscp value] [established] [fin] [flow-label value] [fragments]
[log] [log-input] [neq {port | protocol}] [psh] [range {port | protocol}] [routing] [rst]
[sequence value] [syn] [time-range name] [urg]
```

User Datagram Protocol

```
deny udp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [dscp value] [flow-label value] [fragments] [log] [log-input] [neq
{port | protocol}] [range {port | protocol}] [routing] [sequence value] [time-range name]
```

Syntax Description

| | |
|---|--|
| <i>protocol</i> | Name or number of an Internet protocol. It can be one of the keywords ahp , esp , icmp , ipv6 , pcp , sctp , tcp , or udp , or an integer in the range from 0 to 255 representing an IPv6 protocol number. |
| <i>source-ipv6-prefix/prefix-length</i> | The source IPv6 network or class of networks about which to set deny conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| any | An abbreviation for the IPv6 prefix ::/0. |
| host <i>source-ipv6-address</i> | The source IPv6 host address about which to set deny conditions. This <i>source-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |

| | |
|--|--|
| <i>operator</i> [<i>port-number</i>] | <p>(Optional) Specifies an operand that compares the source or destination ports of the specified protocol. Operands are lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).</p> <p>If the operator is positioned after the <i>source-ipv6-prefix/prefix-length</i> argument, it must match the source port.</p> <p>If the operator is positioned after the <i>destination-ipv6-prefix/prefix-length</i> argument, it must match the destination port.</p> <p>The range operator requires two port numbers. All other operators require one port number.</p> <p>The optional <i>port-number</i> argument is a decimal number or the name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.</p> |
| <i>destination-ipv6-prefix/prefix-length</i> | <p>The destination IPv6 network or class of networks about which to set deny conditions.</p> <p>This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</p> |
| host <i>destination-ipv6-address</i> | <p>The destination IPv6 host address about which to set deny conditions.</p> <p>This <i>destination-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</p> |
| dscp <i>value</i> | <p>(Optional) Matches a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.</p> |
| flow-label <i>value</i> | <p>(Optional) Matches a flow label value against the flow label value in the Flow Label field of each IPv6 packet header. The acceptable range is from 0 to 1048575.</p> |
| fragments | <p>(Optional) Matches non-initial fragmented packets where the fragment extension header contains a non-zero fragment offset. The fragments keyword is an option only if the <i>operator</i> [<i>port-number</i>] arguments are not specified.</p> |
| log | <p>(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the logging console command.)</p> <p>The message includes the access list name and sequence number, whether the packet was denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets denied in the prior 5-minute interval.</p> |
| log-input | <p>(Optional) Provides the same function as the log keyword, except that the logging message also includes the input interface.</p> |
| routing | <p>(Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header.</p> |
| sequence <i>value</i> | <p>(Optional) Specifies the sequence number for the access list statement. The acceptable range is from 1 to 4294967295.</p> |

| | |
|--|--|
| time-range <i>name</i> | (Optional) Specifies the time range that applies to the deny statement. The name of the time range and its restrictions are specified by the time-range and absolute or periodic commands, respectively. |
| undetermined-transport | (Optional) Matches packets from a source for which the Layer 4 protocol cannot be determined. The undetermined-transport keyword is an option only if the <i>operator</i> [<i>port-number</i>] arguments are not specified. |
| <i>icmp-type</i> | (Optional) Specifies an ICMP message type for filtering ICMP packets. ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255. |
| <i>icmp-code</i> | (Optional) Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255. |
| <i>icmp-message</i> | (Optional) Specifies an ICMP message name for filtering ICMP packets. ICMP packets can be filtered by an ICMP message name or ICMP message type and code. The possible names are listed in the “Usage Guidelines” section. |
| ack | (Optional) For the TCP protocol only: acknowledgment (ACK) bit set. |
| established | (Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection. |
| fin | (Optional) For the TCP protocol only: Fin bit set; no more data from sender. |
| neq { <i>port</i> <i>protocol</i> } | (Optional) Matches only packets that are not on a given port number. |
| psh | (Optional) For the TCP protocol only: Push function bit set. |
| range { <i>port</i> <i>protocol</i> } | (Optional) Matches only packets in the range of port numbers. |
| rst | (Optional) For the TCP protocol only: Reset bit set. |
| syn | (Optional) For the TCP protocol only: Synchronize bit set. |
| urg | (Optional) For the TCP protocol only: Urgent pointer bit set. |

Defaults

No IPv6 access list is defined.

Command Modes

IPv6 access list configuration

Command History

| Release | Modification |
|-----------|---|
| 12.0(23)S | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **deny** (IPv6) command is similar to the **deny** (IP) command, except that it is IPv6-specific.

Use the **deny** (IPv6) command following the **ipv6 access-list** command to define the conditions under which a packet passes the access list or to define the access list as a reflexive access list.

Specifying IPv6 for the *protocol* argument matches against the IPv6 header of the packet.

By default, the first statement in an access list is number 10, and the subsequent statements are numbered in increments of 10.

You can add **permit**, **deny**, **remark**, or **evaluate** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

In Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, and 12.0(22)S, IPv6 access control lists (ACLs) are defined and their deny and permit conditions are set by using the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode. In Cisco IOS Release 12.0(23)S or later releases, IPv6 ACLs are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Refer to the **ipv6 access-list** command for more information on defining IPv6 ACLs.



Note

In Cisco IOS Release 12.0(23)S or later releases, every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect.

The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Both the *source-ipv6-prefix/prefix-length* and *destination-ipv6-prefix/prefix-length* arguments are used for traffic filtering (the source prefix filters traffic based upon the traffic source; the destination prefix filters traffic based upon the traffic destination).



Note

IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

The **fragments** keyword is an option only if the *operator [port-number]* arguments are not specified.

The **undetermined-transport** keyword is an option only if the *operator [port-number]* arguments are not specified.

The following is a list of ICMP message names:

- beyond-scope
- destination-unreachable
- echo-reply
- echo-request
- header
- hop-limit
- mld-query
- mld-reduction
- mld-report

- nd-na
- nd-ns
- next-header
- no-admin
- no-route
- packet-too-big
- parameter-option
- parameter-problem
- port-unreachable
- reassembly-timeout
- renum-command
- renum-result
- renum-seq-number
- router-advertisement
- router-renumbering
- router-solicitation
- time-exceeded
- unreachable

Examples

The following example configures the IPv6 access list named toCISCO and applies the access list to outbound traffic on Ethernet interface 0. Specifically, the first deny entry in the list keeps all packets that have a destination TCP port number greater than 5000 from exiting out of Ethernet interface 0. The second deny entry in the list keeps all packets that have a source UDP port number less than 5000 from exiting out of Ethernet interface 0. The second deny also logs all matches to the console. The first permit entry in the list permits all ICMP packets to exit out of Ethernet interface 0. The second permit entry in the list permits all other traffic to exit out of Ethernet interface 0. The second permit entry is necessary because an implicit deny all condition is at the end of each IPv6 access list.

```
ipv6 access-list toCISCO
deny tcp any any gt 5000
deny ::/0 lt 5000 ::/0 log
permit icmp any any
permit any any

interface ethernet 0
ipv6 traffic-filter toCISCO out
```

Related Commands

| Command | Description |
|------------------------------|---|
| ipv6 access-list | Defines an IPv6 access list and enters IPv6 access list configuration mode. |
| ipv6 traffic-filter | Filters incoming or outgoing IPv6 traffic on an interface. |
| permit (IPv6) | Sets permit conditions for an IPv6 access list. |
| show ipv6 access-list | Displays the contents of all current IPv6 access lists. |

dialer-list protocol

To define a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list, use the **dialer-list protocol** command in global configuration mode. To delete a dialer list, use the **no** form of this command.

```
dialer-list dialer-group protocol protocol-name {permit | deny | list access-list-number | access-group}
```

```
no dialer-list dialer-group [protocol protocol-name [list access-list-number | access-group]]
```

| | | |
|---------------------------|---------------------------|---|
| Syntax Description | <i>dialer-group</i> | Number of a dialer access group identified in any dialer-group interface configuration command. |
| | <i>protocol-name</i> | One of the following protocol keywords: appletalk , bridge , clns , clns_es , clns_is , decnet , decnet_router-L1 , decnet_router-L2 , decnet_node , ip , ipx , ipv6 , vines , or xns . |
| | permit | Permits access to an entire protocol. |
| | deny | Denies access to an entire protocol. |
| | list | Specifies that an access list will be used for defining a granularity finer than an entire protocol. |
| | <i>access-list-number</i> | Access list numbers specified in any DECnet, Banyan VINES, IP, Novell IPX, or XNS standard or extended access lists, including Novell IPX extended service access point (SAP) access lists and bridging types, and IPv6 access lists. See Table 17 for the supported access list types and numbers. |
| | <i>access-group</i> | Filter list name used in the clns filter-set and clns access-group commands. |

Defaults No dialer lists are defined.

Command Modes Global configuration

| | | |
|------------------------|----------------|--|
| Command History | Release | Modification |
| | 10.0 | This command was introduced. |
| | 10.3 | The following keyword and arguments were added: <ul style="list-style-type: none"> list <i>access-list-number</i> and <i>access-group</i> |
| | 12.2(2)T | The ipv6 protocol keyword was added. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines The various **no** forms of this command have the following effects:

- The **no dialer-list 1** command deletes all lists configured with list 1, regardless of the keyword previously used (**permit**, **deny**, **protocol**, or **list**).
- The **no dialer-list 1 protocol protocol-name** command deletes all lists configured with list 1 and **protocol protocol-name**.
- The **no dialer-list 1 protocol protocol-name list access-list-number** command deletes the specified list.

The **dialer-list protocol** command permits or denies access to an entire protocol. The **dialer-list protocol list** command provides a finer permission granularity and also supports protocols that were not previously supported.

The **dialer-list protocol list** command applies protocol access lists to dialer access groups to control dialing using DDR. The dialer access groups are defined with the **dialer-group** command.

Table 17 lists the access list types and number range that the **dialer-list protocol list** command supports. The table does not include International Organization for Standardization (ISO) Connectionless Network Services (CLNS) or IPv6 because those protocols use filter names instead of predefined access list numbers.

Table 17 *dialer-list protocol Command Supported Access List Types and Number Range*

| Access List Type | Access List Number Range (Decimal) |
|-------------------------|------------------------------------|
| AppleTalk | 600 to 699 |
| Banyan VINES (standard) | 1 to 100 |
| Banyan VINES (extended) | 101 to 200 |
| DECnet | 300 to 399 |
| IP (standard) | 1 to 99 |
| IP (extended) | 100 to 199 |
| Novell IPX (standard) | 800 to 899 |
| Novell IPX (extended) | 900 to 999 |
| Transparent Bridging | 200 to 299 |
| XNS | 500 to 599 |

Examples

Dialing occurs when an interesting packet (one that matches access list specifications) needs to be output on an interface. Using the standard access list method, packets can be classified as interesting or uninteresting. In the following example, Integrated Gateway Routing Protocol (IGRP) TCP/IP routing protocol updates are not classified as interesting and do not initiate calls:

```
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
```

The following example classifies all other IP packets as interesting and permits them to initiate calls:

```
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

Then the following command places list 101 into dialer access group 1:

```
dialer-list 1 protocol ip list 101
```

In the following example, DECnet access lists allow any DECnet packets with source area 10 and destination area 20 to trigger calls:

```
access-list 301 permit 10.0 0.1023 10.0 0.1023
```



```
access-list 301 permit 10.0 0.1023 20.0 0.1023
```

Then the following command places access list 301 into dialer access group 1:

```
dialer-list 1 protocol decnet list 301
```

In the following example, both IP and VINES access lists are defined. The IP access lists define IGRP packets as uninteresting, but permits all other IP packets to trigger calls. The VINES access lists do not allow Routing Table Protocol (RTP) routing updates to trigger calls, but allow any other data packets to trigger calls.

```
access-list 101 deny igmp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
!
vines access-list 107 deny RTP 00000000:0000 FFFFFFFF:FFFF 00000000:0000 FFFFFFFF:FFFF
vines access-list 107 permit IP 00000000:0000 FFFFFFFF:FFFF 00000000:0000 FFFFFFFF:FFFF
```

Then the following two commands place the IP and VINES access lists into dialer access group 1:

```
dialer-list 1 protocol ip list 101
dialer-list 1 protocol vines list 107
```

In the following example, a CLNS filter is defined and then the filter is placed in dialer access group 1:

```
clns filter-set ddrline permit 47.0004.0001....
!
dialer-list 1 protocol clns list ddrline
```

The following example configures an IPv6 access list named list2 and places the access list in dialer access group 1:

```
ipv6 access-list list2 deny fec0:0:0:2::/64 any
ipv6 access-list list2 permit any any
!
dialer-list 1 protocol ipv6 list list2
```

Related Commands

| Command | Description |
|--------------------------|--|
| access-list | Configures the access list mechanism for filtering frames by protocol type or vendor code. |
| clns filter-set | Builds a list of CLNS address templates with associated permit and deny conditions for use in CLNS filter expressions. |
| dialer-group | Controls access by configuring an interface to belong to a specific dialing group. |
| ipv6 access-list | Defines an IPv6 access list and sets deny or permit conditions for the defined access list. |
| vines access-list | Creates a VINES access list. |

distance (IPv6)

To configure an administrative distance for Intermediate System-to-Intermediate System (IS-IS) or Routing Information Protocol (RIP) IPv6 routes inserted into the IPv6 routing table, use the **distance** command in address family configuration or router configuration mode. To return the administrative distance to its default setting, use the **no** form of this command.

distance *value*

no distance *value*

Syntax Description

| | |
|--------------|--|
| <i>value</i> | The administrative distance. An integer from 10 to 254. (The values 0 to 9 are reserved for internal use. Routes with a distance value of 255 are not installed in the routing table.) |
|--------------|--|

Defaults

IS-IS: 115
RIP: 120

Command Modes

Address family configuration
Router configuration

Command History

| Release | Modification |
|------------|---|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was implemented on the Cisco 12000 series Internet routers, and support for IS-IS was added. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **distance** (IPv6) command is similar to the **distance** (IP) command, except that it is IPv6-specific.

If two processes attempt to insert the same route into the same routing table, the one with the lower administrative distance takes precedence.

An administrative distance is an integer from 10 to 254. 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. Distance values are subjective; there is no quantitative method for choosing the values.

Examples

The following example configures an administrative distance of 190 for the IPv6 IS-IS routing process named area01:

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6
Router(config-router-af)# distance 190
```

The following example configures an administrative distance of 200 for the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco  
Router(config-router)# distance 200
```

distance bgp (IPv6)

To allow the use of external, internal, and local administrative distances that could be a better route than other external, internal, or local routes to a node, use the **distance bgp** command in address family configuration mode. To return to the default values, 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. Acceptable values are from 1 to 255. The default is 20. 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. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table. |
| | <i>local-distance</i> | Administrative distance for BGP local routes. Local routes are those networks listed with a network router configuration command, often as back doors, for that router or for networks that are being redistributed from another process. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table. |

| | |
|----------|--------------------------------|
| Defaults | <i>external-distance</i> : 20 |
| | <i>internal-distance</i> : 200 |
| | <i>local-distance</i> : 200 |

| | |
|---------------|------------------------------|
| Command Modes | Address family configuration |
|---------------|------------------------------|

| | | |
|-----------------|-----------|---|
| Command History | Release | Modification |
| | 12.2(13)T | This command was introduced. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

| | |
|------------------|--|
| Usage Guidelines | The distance bgp (IPv6) command is similar to the distance bgp command, except that it is IPv6-specific. Settings configured by the distance bgp (IPv6) command will override the default IPv6 distance settings. IPv6 BGP is not influenced by the distance settings configured in IPv4 BGP router mode. |
|------------------|--|

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 a positive integer from 1 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Distance values are subjective; there is no quantitative method for choosing the values.

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

For IPv6 multicast BGP (MBGP) distance, the distance assigned is used in reverse path forwarding (RPF) lookup. Use the **show ipv6 rpf** command to display the distance assigned.



Caution

Changing the administrative distance of BGP internal routes is considered dangerous to the system and is not recommended. One problem that can arise is the accumulation of routing table inconsistencies, which can break routing.

Examples

In the following address family configuration mode example, internal routes are known to be preferable to those learned through Interior Gateway Protocol (IGP), so the IPv6 BGP administrative distance values are set accordingly:

```
router bgp 65001
 neighbor 2001:0DB8::1 remote-as 65002
 address-family ipv6
  distance bgp 20 20 200
 neighbor 2001:0DB8::1 activate
 exit-address-family
```

Related Commands

| Command | Description |
|----------------------|---|
| show ipv6 rpf | Displays RPF information for a given unicast host address and prefix. |

distribute-list prefix-list (IPv6 RIP)

To apply a prefix list to IPv6 Routing Information Protocol (RIP) routing updates that are received or sent on an interface, use the **distribute-list prefix-list** command in router configuration mode. To remove the prefix list, use the **no** form of this command.

distribute-list prefix-list *word* {**in** | **out**} [*interface-type interface-number*]

no distribute-list prefix-list *word*

Syntax Description

| | |
|-------------------------|---|
| <i>word</i> | Name of a prefix list. The list defines which IPv6 RIP networks are to be accepted in incoming routing updates and which networks are to be advertised in outgoing routing updates, based upon matching the network prefix to the prefixes in the list. |
| in | Applies the prefix list to incoming routing updates on the specified interface. |
| out | Applies the prefix list to outgoing routing updates on the specified interface. |
| <i>interface-type</i> | (Optional) The specified interface type. For supported interface types, use the question mark (?) online help function. |
| <i>interface-number</i> | (Optional) The specified interface number. |

Defaults

Prefix lists are not applied to IPv6 RIP routing updates.

Command Modes

Router configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

If no interface is specified, the prefix list is applied to all interfaces.

Examples

The following example applies the prefix list named cisco to IPv6 RIP routing updates that are received on Ethernet interface 0/0:

```
Router(config)# ipv6 router rip cisco
Router(config-rtr-rip)# distribute-list prefix-list cisco in ethernet 0/0
```

Related Commands

| Command | Description |
|------------------------------|--|
| ipv6 prefix-list | Creates an entry in an IPv6 prefix list. |
| show ipv6 prefix-list | Displays information about an IPv6 prefix list or prefix list entries. |

dns-server (IPv6)

To specify the Domain Name System (DNS) IPv6 servers available to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **dns-server** command in DHCP for IPv6 pool configuration mode. To remove the DNS server list, use the **no** form of this command.

dns-server *ipv6-address*

no dns-server *ipv6-address*

Syntax Description

ipv6-address

The IPv6 address of a DNS server.

This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Defaults

When a DHCP for IPv6 pool is first created, no DNS IPv6 servers are configured.

Command Modes

DHCP for IPv6 pool configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.3(4)T | This command was introduced. |

Usage Guidelines

Multiple Domain Name System (DNS) server addresses can be configured by issuing this command multiple times. New addresses will not overwrite old addresses.

Examples

The following example specifies the DNS IPv6 servers available:

```
dns-server 2001:0DB8:3000:3000::42
```

Related Commands

| Command | Description |
|-----------------------|---|
| domain-name | Configures a domain name for a DHCP for IPv6 client. |
| ipv6 dhcp pool | Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode. |

domain-name (IPv6)

To configure a domain name for a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **domain-name** command in DHCP for IPv6 pool configuration mode. To remove the domain name, use the **no** form of this command.

domain-name *domain*

no domain-name

Syntax Description

| | |
|---------------|--|
| <i>domain</i> | Specifies the domain name string to be used by the client. |
|---------------|--|

Defaults

When a DHCP for IPv6 pool is first created, no domain name for clients is configured.

Command Modes

DHCP for IPv6 pool configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.3(4)T | This command was introduced. |

Usage Guidelines

Multiple Domain Name System (DNS) domain names can be configured by issuing the **domain-name** command multiple times. The new domain name will not overwrite existing domain names.

Examples

The following example specifies domain1.com as the domain name to be used by clients:

```
domain-name domain1.com
```

Related Commands

| Command | Description |
|-----------------------|---|
| dns-server | Specifies the DNS IPv6 servers available to a DHCP for IPv6 client. |
| ipv6 dhcp pool | Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode. |

evaluate (IPv6)

To nest an IPv6 reflexive access list within an IPv6 access list, use the **evaluate** (IPv6) command in IPv6 access list configuration mode. To remove the nested IPv6 reflexive access list from the IPv6 access list, use the **no** form of this command.

evaluate *access-list-name* [**sequence** *value*]

no evaluate *access-list-name* [**sequence** *value*]

Syntax Description

| | |
|------------------------------|--|
| <i>access-list-name</i> | The name of the IPv6 reflexive access list that you want evaluated for IPv6 traffic entering your internal network. This is the name defined in the permit (IPv6) command. Names cannot contain a space or quotation mark, or begin with a numeric. |
| sequence <i>value</i> | (Optional) Specifies the sequence number for the IPv6 reflexive access list. The acceptable range is from 1 to 4294967295. |

Defaults

IPv6 reflexive access lists are not evaluated.

Command Modes

IPv6 access list configuration

Command History

| Release | Modification |
|-----------|---|
| 12.0(23)S | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **evaluate** (IPv6) command is similar to the **evaluate** (IPv4) command, except that it is IPv6-specific. This command is used to achieve IPv6 reflexive filtering, a form of session filtering.

Before this command will work, you must define the IPv6 reflexive access list using the **permit** (IPv6) command.

This command nests an IPv6 reflexive access list within an IPv6 access control list (ACL).

If you are configuring an IPv6 reflexive access list for an external interface, the IPv6 ACL should be one that is applied to inbound traffic. If you are configuring IPv6 reflexive access lists for an internal interface, the IPv6 ACL should be one that is applied to outbound traffic. (In other words, use the access list opposite of the one used to define the IPv6 reflexive access list.)

This command allows IPv6 traffic entering your internal network to be evaluated against the reflexive access list. Use this command as an entry (condition statement) in the IPv6 ACL; the entry “points” to the IPv6 reflexive access list to be evaluated.

As with all IPv6 ACL entries, the order of entries is important. Normally, when a packet is evaluated against entries in an IPv6 ACL, the entries are evaluated in sequential order, and when a match occurs, no more entries are evaluated. With an IPv6 reflexive access list nested in an IPv6 ACL, the IPv6 ACL

entries are evaluated sequentially up to the nested entry, then the IPv6 reflexive access list entries are evaluated sequentially, and then the remaining entries in the IPv6 ACL are evaluated sequentially. As usual, after a packet matches any of these entries, no more entries will be evaluated.

**Note**

IPv6 reflexive access lists do not have any implicit deny or implicit permit statements.

Examples

The **evaluate** command in the following example nests the temporary IPv6 reflexive access lists named TCPTRAFFIC and UDPTRAFFIC in the IPv6 ACL named OUTBOUND. The two reflexive access lists are created dynamically (session filtering is “triggered”) when incoming TCP or UDP traffic matches the applicable permit entry in the IPv6 ACL named INBOUND. The OUTBOUND IPv6 ACL uses the temporary TCPTRAFFIC or UDPTRAFFIC access list to match (evaluate) outgoing TCP or UDP traffic related to the triggered session. The TCPTRAFFIC and UDPTRAFFIC lists time out automatically when no IPv6 packets match the permit statement that triggered the session (the creation of the temporary reflexive access list).

**Note**

The order of IPv6 reflexive access list entries is not important because only permit statements are allowed in IPv6 reflexive access lists and reflexive access lists do not have any implicit conditions. The OUTBOUND IPv6 ACL simply evaluates the UDPTRAFFIC reflexive access list first and, if there were no matches, the TCPTRAFFIC reflexive access list second. Refer to the **permit** command for more information on configuring IPv6 reflexive access lists.

```
ipv6 access-list INBOUND
  permit tcp any any eq bgp reflect TCPTRAFFIC
  permit tcp any any eq telnet reflect TCPTRAFFIC
  permit udp any any reflect UDPTRAFFIC

ipv6 access-list OUTBOUND
  evaluate UDPTRAFFIC
  evaluate TCPTRAFFIC
```

Related Commands

| Command | Description |
|------------------------------|---|
| ipv6 access-list | Defines an IPv6 access list and enters IPv6 access list configuration mode. |
| permit (IPv6) | Sets permit conditions for an IPv6 access list. |
| show ipv6 access-list | Displays the contents of all current IPv6 access lists. |

frame-relay map ipv6

To define the mapping between a destination IPv6 address and the data-link connection identifier (DLCI) used to connect to the destination address, use the **frame-relay map ipv6** command in interface configuration mode. To delete the map entry, use the **no** form of this command.

```
frame-relay map ipv6 ipv6-address dlci [broadcast] [cisco] [ietf] [payload-compression
{packet-by-packet | frf9 stac [hardware-options] | data-stream stac [hardware-options]}]
```

```
no frame-relay map ipv6 ipv6-address
```

| Syntax Description | | |
|--------------------|----------------------------|---|
| | <i>ipv6-address</i> | Destination IPv6 (protocol) address that is being mapped to a permanent virtual circuit (PVC). 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>dlci</i> | DLCI number used to connect to the specified protocol address on the interface. The acceptable range is from 16 to 1007. |
| | broadcast | (Optional) Forwards IPv6 multicast packets to this address when multicast is not enabled (see the frame-relay multicast-dlci command for more information about multicasts). Note IPv6 supports multicast packets; broadcast packets are not supported. |
| | cisco | (Optional) Cisco encapsulation method. |
| | ietf | (Optional) Internet Engineering Task Force (IETF) Frame Relay encapsulation method. Used when the router or access server is connected to the equipment of another vendor across a Frame Relay network. |
| | payload-compression | (Optional) Enables payload compression. |
| | packet-by-packet | (Optional) Packet-by-packet payload compression using the Stacker method. |
| | frf9 stac | (Optional) FRF.9 compression using the Stacker method: <ul style="list-style-type: none"> • If the router contains a compression service adapter (CSA), compression is performed in the CSA hardware (hardware compression). • If the CSA is not available, compression is performed in the software installed on the Versatile Interface Processor (VIP2) (distributed compression). • If the second-generation VIP2 is not available, compression is performed in the main processor of the router (software compression). |

| | |
|-------------------------|--|
| data-stream stac | (Optional) Data-stream compression using the Stacker method: <ul style="list-style-type: none"> • If the router contains a CSA, compression is performed in the CSA hardware (hardware compression). • If the CSA is not available, compression is performed in the main processor of the router (software compression). |
| <i>hardware-options</i> | (Optional) Choose one of the following hardware options: <ul style="list-style-type: none"> • distributed—Specifies that compression is implemented in the software that is installed in the VIP2. If the VIP2 is not available, compression is performed in the main processor of the router (software compression). This option applies only to the Cisco 7500 series routers. This option is not supported with data-stream compression. • software—Specifies that compression is implemented in the Cisco IOS software installed in the main processor of the router. • csa csa_number—Specifies the CSA to use for a particular interface. This option applies only to Cisco 7200 series routers. |

Defaults

No mapping is defined.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **frame-relay map ipv6** command is similar to the **frame-relay map** command, except that it is IPv6-specific.

Many DLCIs can be known by a router or access server and can send data to many different places, but they are all multiplexed over one physical link. The Frame Relay map defines the logical connection between a specific protocol and address pair and the correct DLCI.

The optional **ietf** and **cisco** keywords allow flexibility in the configuration. If no keywords are specified, the map inherits the attributes set with the **encapsulation frame-relay** command. You can also use the encapsulation options to specify that, for example, all interfaces use IETF encapsulation except one, which needs the original Cisco encapsulation method and can be configured through use of the **cisco** keyword with the **frame-relay map ipv6** command.

Data-stream compression is supported on interfaces and virtual circuits (VCs) using Cisco proprietary encapsulation. When the **data-stream stac** keywords are specified, Cisco encapsulation is automatically enabled. FRF.9 compression is supported on IETF-encapsulated VCs and interfaces. When the **frf9 stac** keywords are specified, IETF encapsulation is automatically enabled.

Packet-by-packet compression is Cisco-proprietary and will not interoperate with routers of other manufacturers.

You can disable payload compression by entering the **no frame-relay map ipv6 payload-compression** command and then entering the **frame-relay map ipv6** command again with one of the other encapsulation keywords (**ietf** or **cisco**).

Use the **frame-relay map ipv6** command to enable or disable payload compression on multipoint interfaces. Use the **frame-relay payload-compression** command to enable or disable payload compression on point-to-point interfaces.

We recommend that you shut down the interface before changing encapsulation types. Although not required, shutting down the interface ensures that the interface is reset for the new encapsulation.

Examples

In the following example, three nodes named Cisco A, Cisco B, and Cisco C make up a fully meshed network. Each node is configured with two PVCs, which provide an individual connection to each of the other two nodes. Each PVC is configured on a different point-to-point subinterface, which creates three unique IPv6 networks (2001:0DB8:2222:1017::/64, 2001:0DB8:2222:1018::/64, and 2001:0DB8:2222:1019::/64). Therefore, the mappings between the IPv6 addresses of each node and the DLCI (DLCI 17, 18, and 19) of the PVC used to reach the addresses are implicit (no additional mappings are required).



Note

Given that each PVC in the following example is configured on a different point-to-point subinterface, the configuration in the following example can also be used in a network that is not fully meshed. Additionally, configuring each PVC on a different point-to-point subinterface can help simplify your routing protocol configuration. However, the configuration in the following example requires more than one IPv6 network, whereas configuring each PVC on point-to-multipoint interfaces requires only one IPv6 network.

Cisco A Configuration

```
interface Serial3
 encapsulation frame-relay
 !
interface Serial3.17 point-to-point
 description to Cisco B
 ipv6 address 2001:0DB8:2222:1017::46/64
 frame-relay interface-dlci 17
 !
interface Serial3.19 point-to-point
 description to Cisco C
 ipv6 address 2001:0DB8:2222:1019::46/64
 frame-relay interface-dlci 19
```

Cisco B Configuration

```
interface Serial5
 encapsulation frame-relay
 !
interface Serial5.17 point-to-point
 description to Cisco A
 ipv6 address 2001:0DB8:2222:1017::73/64
 frame-relay interface-dlci 17
 !
interface Serial5.18 point-to-point
 description to Cisco C
 ipv6 address 2001:0DB8:2222:1018::73/64
```

```
frame-relay interface-dlci 18
```

Cisco C Configuration

```
interface Serial0
  encapsulation frame-relay
!
interface Serial0.18 point-to-point
  description to Cisco B
  ipv6 address 2001:0DB8:2222:1018::72/64
  frame-relay interface-dlci 18
!
interface Serial0.19 point-to-point
  description to Cisco A
  ipv6 address 2001:0DB8:2222:1019::72/64
  frame-relay interface-dlci 19
```

In the following example, the same three nodes (Cisco A, Cisco B, and Cisco C) from the previous example make up a fully meshed network and each node is configured with two PVCs (which provide an individual connection to each of the other two nodes). However, the two PVCs on each node in the following example are configured on a single interface (serial 3, serial 5, and serial 10, respectively), which makes each interface a point-to-multipoint interface. Therefore, explicit mappings are required between the link-local and global IPv6 addresses of each interface on all three nodes and the DLCI (DLCI 17, 18, and 19) of the PVC used to reach the addresses.

Cisco A Configuration

```
interface Serial3
  encapsulation frame-relay
  ipv6 address 2001:0DB8:2222:1044::46/64
  frame-relay map ipv6 FE80::E0:F727:E400:A 17 broadcast
  frame-relay map ipv6 FE80::60:3E47:AC8:8 19 broadcast
  frame-relay map ipv6 2001:0DB8:2222:1044::72 19
  frame-relay map ipv6 2001:0DB8:2222:1044::73 17
```

Cisco B Configuration

```
interface Serial5
  encapsulation frame-relay
  ipv6 address 2001:0DB8:2222:1044::73/64
  frame-relay map ipv6 FE80::60:3E59:DA78:C 17 broadcast
  frame-relay map ipv6 FE80::60:3E47:AC8:8 18 broadcast
  frame-relay map ipv6 2001:0DB8:2222:1044::46 17
  frame-relay map ipv6 2001:0DB8:2222:1044::72 18
```

Cisco C Configuration

```
interface Serial0
  encapsulation frame-relay
  ipv6 address 2001:0DB8:2222:1044::72/64
  frame-relay map ipv6 FE80::60:3E59:DA78:C 19 broadcast
  frame-relay map ipv6 FE80::E0:F727:E400:A 18 broadcast
  frame-relay map ipv6 2001:0DB8:2222:1044::46 19
  frame-relay map ipv6 2001:0DB8:2222:1044::73 18
```

Related Commands

| Command | Description |
|-------------------------------------|--|
| encapsulation frame-relay | Enables Frame Relay encapsulation. |
| frame-relay payload-compress | Enables Stacker payload compression on a specified point-to-point interface or subinterface. |

ip name-server

To specify the address of one or more name servers to use for name and address resolution, use the **ip name-server** command in global configuration mode. To remove the addresses specified, use the **no** form of this command.

ip name-server *server-address1* [*server-address2...server-address6*]

no ip name-server *server-address1* [*server-address2...server-address6*]

| | | |
|---------------------------|--|---|
| Syntax Description | <i>server-address1</i> | IPv4 or IPv6 addresses of a name server. |
| | <i>server-address2...server-address6</i> | (Optional) IP addresses of additional name servers (a maximum of six name servers). |

Defaults No name server addresses are specified.

Command Modes Global configuration

| Command History | Release | Modification |
|------------------------|--|---------------------------------------|
| | 10.0 | This command was introduced. |
| | 12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S | Support for IPv6 addresses was added. |
| | | |

Examples The following example specifies IPv4 hosts 172.16.1.111 and 172.16.1.2 as the name servers:

```
ip name-server 172.16.1.111 172.16.1.2
```

This command will be reflected in the configuration file as follows:

```
ip name-server 172.16.1.111
ip name-server 172.16.1.2
```

The following example specifies IPv6 hosts 3FFE:C00::250:8BFF:FEE8:F800 and 2001:0DB8::3 as the name servers:

```
ip name-server 3FFE:C00::250:8BFF:FEE8:F800 2001:0DB8::3
```

This command will be reflected in the configuration file as follows:

```
ip name-server 3FFE:C00::250:8BFF:FEE8:F800
ip name-server 2001:0DB8::3
```

| Related Commands | Command | Description |
|-------------------------|-------------------------|--|
| | ip domain-lookup | Enables the IP DNS-based host name-to-address translation. |
| | ip domain-name | Defines a default domain name to complete unqualified host names (names without a dotted decimal domain name). |

ipv6 access-class

To filter incoming and outgoing connections to and from the router based on an IPv6 access list, use the **ipv6 access-class** command in line configuration mode. To disable the filtering of incoming and outgoing connections to the router, use the **no** form of this command.

ipv6 access-class *ipv6-access-list-name* { **in** | **out** }

no ipv6 access-class

Syntax Description

| | |
|------------------------------|---|
| <i>ipv6-access-list-name</i> | Name of an IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric. |
| in | Filters incoming IPv6 connections. |
| out | Filters outgoing IPv6 connections. |

Defaults

The filtering of incoming and outgoing connections to and from the router is not enabled.

Command Modes

Line configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **ipv6 access-class** command is similar to the **access-class** command, except that it is IPv6-specific. The incoming connection source address is used to match against the access list source prefix. The router address on the received interface is used to match against the access list destination prefix.

IPv6 access control list (ACL) matches are made using TCP; an ACL permit match using IPv6 or TCP is required to allow access to a router.

Examples

The following example filters incoming connections on virtual terminal lines 0 to 4 of the router based on the IPv6 access list named cisco:

```

ipv6 access-list cisco
 permit ipv6 host 2001:0DB8:0:4::2/128 any

line vty 0 4
 ipv6 access-class cisco in
  
```

Related Commands

| Command | Description |
|-----------------------|---|
| ipv6 access-list | Defines an IPv6 access list and sets deny or permit conditions for the defined access list. |
| ipv6 traffic-filter | Filters incoming or outgoing IPv6 traffic on an interface. |
| show ipv6 access-list | Displays the contents of all current IPv6 access lists. |

ipv6 access-list

To define an IPv6 access list and to place the router in IPv6 access list configuration mode, use the **ipv6 access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

ipv6 access-list *access-list-name*

no ipv6 access-list *access-list-name*

| | | |
|---------------------------|-------------------------|--|
| Syntax Description | <i>access-list-name</i> | Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric. |
|---------------------------|-------------------------|--|

| | |
|-----------------|---------------------------------|
| Defaults | No IPv6 access list is defined. |
|-----------------|---------------------------------|

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| Command History | Release | Modification |
|-----------------|----------------------|---|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.0(23)S, 12.2(13)T | Support for IPv6 address configuration mode and extended access list functionality (the filtering of traffic based on IPv6 option headers and optional, upper-layer protocol type information) was added. Additionally, the following keywords and arguments were moved from global configuration mode to IPv6 access list configuration mode: permit , deny , <i>source-ipv6-prefix/prefix-length</i> , any , <i>destination-ipv6-prefix/prefix-length</i> , priority . See the “Usage Guidelines” section for more details. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

| | |
|-------------------------|--|
| Usage Guidelines | The ipv6 access-list command is similar to the ip access-list command, except that it is IPv6-specific. |
| | In Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, and 12.0(22)S, standard IPv6 access control list (ACL) functionality is used for basic traffic filtering functions—traffic filtering is based on source and destination addresses, inbound and outbound to a specific interface, and with an implicit deny statement at the end of each access list (functionality similar to standard ACLs in IPv4). IPv6 ACLs are defined and their deny and permit conditions are set by using the ipv6 access-list command with the deny and permit keywords in global configuration mode. |

In Cisco IOS Release 12.0(23)S or later releases, the standard IPv6 ACL functionality is extended to support—in addition to traffic filtering based on source and destination addresses—filtering of traffic based on IPv6 option headers and optional, upper-layer protocol type information for finer granularity of control (functionality similar to extended ACLs in IPv4). IPv6 ACLs are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using

the **deny** and **permit** commands in IPv6 access list configuration mode. Configuring the **ipv6 access-list** command places the router in IPv6 access list configuration mode—the router prompt changes to Router(config-ipv6-acl)#. From IPv6 access list configuration mode, permit and deny conditions can be set for the defined IPv6 ACL.


Note

IPv6 ACLs are defined by a unique name (IPv6 does not support numbered ACLs). An IPv4 ACL and an IPv6 ACL cannot share the same name.

In Cisco IOS Release 12.0(23)S or later releases, and 12.2(11)S or later releases, for backward compatibility, the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode is still supported; however, an IPv6 ACL defined with deny and permit conditions in global configuration mode is translated to IPv6 access list configuration mode.

Refer to the **deny** (IPv6) and **permit** (IPv6) commands for more information on filtering IPv6 traffic based on IPv6 option headers and optional, upper-layer protocol type information. See the “Examples” section for an example of a translated IPv6 ACL configuration.


Note

In Cisco IOS Release 12.0(23)S or later releases, every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect.

The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.


Note

IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

Use the **ipv6 traffic-filter** interface configuration command with the *access-list-name* argument to apply an IPv6 ACL to an IPv6 interface. Use the **ipv6 access-class** line configuration command with the *access-list-name* argument to apply an IPv6 ACL to incoming and outgoing IPv6 virtual terminal connections to and from the router.


Note

An IPv6 ACL applied to an interface with the **ipv6 traffic-filter** command filters traffic that is forwarded, not originated, by the router.

Examples

The following example is from a router running Cisco IOS Release 12.0(23)S or later releases. The example configures the IPv6 ACL list named list1 and places the router in IPv6 access list configuration mode.

```
Router(config)# ipv6 access-list list1
Router(config-ipv6-acl)#
```

The following example is from a router running Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, or 12.0(22)S. The example configures the IPv6 ACL named list2 and applies the ACL to outbound traffic on Ethernet interface 0. Specifically, the first ACL entry keeps all packets from the

network FEC0:0:0:2::/64 (packets that have the site-local prefix FEC0:0:0:2 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0. The second entry in the ACL permits all other traffic to exit out of Ethernet interface 0. The second entry is necessary because an implicit deny all condition is at the end of each IPv6 ACL.

```
Router(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Router(config)# ipv6 access-list list2 permit any any
```

```
Router(config)# interface ethernet 0
Router(config-if)# ipv6 traffic-filter list2 out
```

If the same configuration was entered on a router running Cisco IOS Release 12.0(23)S or later releases, the configuration would be translated into IPv6 access list configuration mode as follows:

```
ipv6 access-list list2
  deny FEC0:0:0:2::/64 any
  permit ipv6 any any

interface ethernet 0
  ipv6 traffic-filter list2 out
```


Note

IPv6 is automatically configured as the protocol type in **permit any any** and **deny any any** statements that are translated from global configuration mode to IPv6 access list configuration mode.


Note

IPv6 ACLs defined on a router running Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, or 12.0(22)S that rely on the implicit deny condition or specify a **deny any any** statement to filter traffic should contain **permit** statements for link-local and multicast addresses to avoid the filtering of protocol packets (for example, packets associated with the neighbor discovery protocol). Additionally, IPv6 ACLs that use **deny** statements to filter traffic should use a **permit any any** statement as the last statement in the list.


Note

An IPv6 router will not forward to another network an IPv6 packet that has a link-local address as either its source or destination address (and the source interface for the packet is different from the destination interface for the packet).

Related Commands

| Command | Description |
|------------------------------|--|
| deny (IPv6) | Sets deny conditions for an IPv6 access list. |
| ipv6 access-class | Filters incoming and outgoing connections to and from the router based on an IPv6 access list. |
| ipv6 traffic-filter | Filters incoming or outgoing IPv6 traffic on an interface. |
| permit (IPv6) | Sets permit conditions for an IPv6 access list. |
| show ipv6 access-list | Displays the contents of all current IPv6 access lists. |

ipv6 access-list log-update threshold

To specify the number of updates that are logged for IPv6 access lists, use the **ipv6 access-list log-update threshold** command in global configuration mode. To return the number of logged updates to the default setting, use the **no** form of this command.

ipv6 access-list log-update threshold *value*

no ipv6 access-list log-update threshold

| | | |
|---------------------------|--------------|--|
| Syntax Description | <i>value</i> | Specifies the number of updates that are logged for every IPv6 access list configured on the router. The acceptable range is from 0 to 2147483647. |
|---------------------------|--------------|--|

| | |
|-----------------|---------------------|
| Defaults | 2147483647 updates. |
|-----------------|---------------------|

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| Command History | Release | Modification |
|------------------------|-----------|---|
| | 12.0(23)S | This command was introduced. |
| | 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

| | |
|-------------------------|--|
| Usage Guidelines | The ipv6 access-list log-update threshold command is similar to the ip access-list log-update threshold command, except that it is IPv6-specific. |
| | IPv6 ACL updates are logged at five minute intervals, following the first logged update. Configuring a lower number of updates (a number lower than the default) is useful when more frequent update logging is desired. |

| | |
|-----------------|--|
| Examples | The following example configures a log threshold of ten updates for every IPv6 access list configured on the router. |
| | <pre>ipv6 access-list log-update threshold 10</pre> |

| Related Commands | Command | Description |
|-------------------------|------------------------------|---|
| | ipv6 access-list | Defines an IPv6 access list and enters IPv6 access list configuration mode. |
| | show ipv6 access-list | Displays the contents of all current IPv6 access lists. |

ipv6 address

To configure an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface, use the **ipv6 address** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address *prefix-name* *ipv6-prefix/prefix-length*

no ipv6 address [*prefix-name* *ipv6-prefix/prefix-length*]

Syntax Description

| | |
|-----------------------|--|
| <i>prefix-name</i> | A general prefix, which specifies the leading bits of the network to be configured on the interface. |
| <i>ipv6-prefix</i> | The subsequent bits of the address to be configured on the interface. 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> | The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |

Defaults

No IPv6 addresses are defined for any interface.

Command Modes

Interface configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.3(4)T | This command was introduced. |

Usage Guidelines

The **ipv6 address** command allows the address to be configured on an interface to be defined in two stages. The leading bits of the address are defined in a general prefix, which is globally configured, and then applied, using the *prefix-name* argument. The subsequent bits are defined directly, using the *ipv6-prefix* argument.

Using the **no ipv6 address** command without arguments removes all manually configured IPv6 addresses from an interface.

Examples

When entered in interface configuration mode, the following example enables IPv6 processing on the interface, and configures an address based on the general prefix called my-prefix and the directly specified bits:

```
Router(config-if) ipv6 address my-prefix 0:0:0:7272::72/64
```

Assuming the general prefix named my-prefix has the value of 2001:DB8:2222::/48, then the interface would be configured with the global address 2001:DB8:2222:7272::72/64.

Related Commands

| Command | Description |
|--------------------------------|--|
| ipv6 address anycast | Configures an IPv6 anycast address and enables IPv6 processing on an interface. |
| ipv6 address eui-64 | Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address. |
| ipv6 address link-local | Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface. |
| ipv6 unnumbered | Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface. |
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 address anycast

To configure an IPv6 anycast address and enable IPv6 processing on an interface, use the **ipv6 address anycast** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-prefix/prefix-length* **anycast**

no ipv6 address [*ipv6-prefix/prefix-length* **anycast**]

| | | |
|---------------------------|-----------------------|--|
| Syntax Description | <i>ipv6-prefix</i> | The IPv6 network assigned to the interface. 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> | The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |

Defaults No IPv6 addresses are defined for any interface.

Command Modes Interface configuration

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 12.3(4)T | This command was introduced. |

Usage Guidelines Using the **no ipv6 address** command without arguments removes all manually configured IPv6 addresses from an interface.

Examples When entered in interface configuration mode, the following example enables IPv6 processing on the interface, assigns the prefix 2001:0DB8:1:1::/64 to the interface, and configures the IPv6 anycast address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE:

```
ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast
```

| | | |
|-------------------------|--------------------------------|--|
| Related Commands | Command | Description |
| | ipv6 address eui-64 | Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address. |
| | ipv6 address link-local | Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface. |

| Command | Description |
|----------------------------|--|
| ipv6 unnumbered | Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface. |
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 address autoconfig

To enable automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enable IPv6 processing on the interface, use the **ipv6 address autoconfig** command in interface configuration mode. Addresses are configured depending on the prefixes received in Router Advertisement messages. To remove the address from the interface, use the **no** form of this command.

ipv6 address autoconfig

no ipv6 address autoconfig

Syntax Description

This command has no keywords or arguments.

Defaults

No IPv6 address is defined for the interface.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-----------|------------------------------|
| 12.2(13)T | This command was introduced. |

Usage Guidelines

If the Cisco IOS software detects another host using one of its IPv6 addresses, it will display an error message on the console.

The system automatically generates a link-local address for an interface when IPv6 processing is enabled on the interface, typically when an IPv6 address is configured on the interface.

If router advertisements (RAs) received on this interface have the “other configuration” flag set, then the interface will also attempt to acquire other configuration (i.e., non-address) using DHCP for IPv6.

Examples

The following example assigns the IPv6 address automatically.

```
Router(config)# interface ethernet 0
Router(config-if)# ipv6 address autoconfig
```

Related Commands

| Command | Description |
|--------------------------------|--|
| ipv6 address eui-64 | Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address. |
| ipv6 address link-local | Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface. |
| ipv6 unnumbered | Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface. |
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 address eui-64

To configure an IPv6 address for an interface and enables IPv6 processing on the interface using an EUI-64 interface ID in the low order 64 bits of the address, use the **ipv6 address eui-64** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-prefix/prefix-length* **eui-64**

no ipv6 address [*ipv6-prefix/prefix-length* **eui-64**]

| | | |
|---------------------------|-----------------------|--|
| Syntax Description | <i>ipv6-prefix</i> | The IPv6 network assigned to the interface. 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>lprefix-length</i> | The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |

Defaults No IPv6 address is defined for the interface.

Command Modes Interface configuration

| Command History | Release | Modification |
|------------------------|----------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

If the value specified for the *lprefix-length* argument is greater than 64 bits, the prefix bits have precedence over the interface ID.

Using the **no ipv6 address** command without arguments removes all manually configured IPv6 addresses from an interface.

If the Cisco IOS software detects another host using one of its IPv6 addresses, it will display an error message on the console.

Examples The following example assigns IPv6 address 2001:0DB8:0:1::/64 to Ethernet interface 0 and specifies an EUI-64 interface ID in the low order 64 bits of the address:

```
Router(config)# interface ethernet 0
Router(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
```

Related Commands

| Command | Description |
|--------------------------------|--|
| ipv6 address link-local | Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface. |
| ipv6 unnumbered | Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface. |
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 address link-local

To configure an IPv6 link-local address for an interface and enable IPv6 processing on the interface, use the **ipv6 address link-local** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-address* **link-local**

no ipv6 address [*ipv6-address* **link-local**]

Syntax Description

| | |
|---------------------|---|
| <i>ipv6-address</i> | The IPv6 address assigned to the interface. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| link-local | Specifies a link-local address. The <i>ipv6-address</i> specified with this command overrides the link-local address that is automatically generated for the interface. |

Defaults

No IPv6 address is defined for the interface.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

Using the **no ipv6 address** command without arguments removes all manually configured IPv6 addresses from an interface.

If the Cisco IOS software detects another host using one of its IPv6 addresses, it will display an error message on the console.

The system automatically generates a link-local address for an interface when IPv6 processing is enabled on the interface, typically when an IPv6 address is configured on the interface. To manually specify a link-local address to be used by an interface, use the **ipv6 address link-local** command.

A double colon may be used as part of the *ipv6-address* argument when consecutive 16-bit values are denoted as zero. You can configure multiple IPv6 addresses per interfaces, but only one link-local address.

Examples

The following example assigns FE80::260:3EFF:FE11:6770 as the link-local address for Ethernet interface 0:

```
interface ethernet 0
  ipv6 address FE80::260:3EFF:FE11:6770 link-local
```

| Related Commands | Command | Description |
|------------------|----------------------------|--|
| | ipv6 address eui-64 | Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address. |
| | ipv6 unnumbered | Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface. |
| | show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 atm-vc

To configure a mapping between a virtual circuit (VC) and the IPv6 address of a system at the far end of that circuit, use the **ipv6 atm-vc** command in map-list configuration mode. To remove the mapping, use the **no** form of this command.

```

ipv6 ipv6-address atm-vc vcd [broadcast]

no ipv6 ipv6-address atm-vc vcd [broadcast]
```

| | | |
|--------------------|---------------------|--|
| Syntax Description | <i>ipv6-address</i> | The IPv6 address of a system at the far end of the specified virtual circuit. 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>vcd</i> | The virtual circuit descriptor for the virtual circuit mapped to the specified IPv6 address. |
| | broadcast | (Optional) Specifies that this map entry is used when sending IPv6 multicast packets to the interface (for example, network routing protocol updates). |


Defaults No default behavior or values.

Command Modes Map-list configuration

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines ATM permanent virtual circuits (PVCs) can be configured in the following modes:

- Nonbroadcast multiaccess (NBMA) mode—A neighbor is mapped to a PVC. ATM point-to-multipoint PVCs are configured using static maps. The **ipv6 atm-vc** command utilizes static maps.
- Point-to point-mode—Each PVC is given a subinterface and is configured as a standard point-to-point link.



Note

We recommend configuring ATM PVCs in point-to-point mode.

Examples

The following example maps neighbor 2001:0DB8::5 to ATM point-to-multipoint PVC 1, virtual path identifier (VPI) 3, and virtual channel identifier (VCI) 5:

```
Router(config)# interface atm 1/0
Router(config-if)# atm pvc 1 3 5 aal5snap
Router(config-if)# map-group cisco

Router(config)# map-list cisco
Router(config-map-list)# ipv6 2001:0DB8::5 atm-vc 1
```

Related Commands

| Command | Description |
|----------------------------|--|
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 cef

To enable Cisco Express Forwarding for IPv6 (CEFv6), use the **ipv6 cef** command in global configuration mode. To disable CEFv6, use the **no** form of this command.

```
ipv6 cef

no ipv6 cef
```

Syntax Description This command has no arguments or keywords.


Defaults CEFv6 is disabled by default.


Command Modes Global configuration


| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(22)S | This command was introduced. |
| | 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines The **ipv6 cef** command is similar to the **ip cef** command, except that it is IPv6-specific.

The **ipv6 cef** command is not available on the Cisco 12000 series Internet routers because this distributed platform operates only in distributed CEFv6 (dCEFv6) mode.

 **Note** The **ipv6 cef** command is not supported in interface configuration mode.

 **Note** Some distributed architecture platforms, such as the Cisco 7500 series routers, support both CEFv6 and dCEFv6. When CEFv6 is configured on distributed platforms, CEF switching is performed by the Route Processor (RP).

 **Note** You must enable CEF for IPv4 (CEFv4) by using the **ip cef** global configuration command before enabling CEFv6 by using the **ipv6 cef** global configuration command.

CEFv6 is advanced Layer 3 IP switching technology that functions the same and offer the same benefits as CEFv4. CEFv6 optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with web-based applications and interactive sessions.

Examples

The following example enables standard CEFv4 operation and then standard CEFv6 operation globally on the router.

```
ip cef
ipv6 cef
```

Related Commands

| Command | Description |
|-----------------------------|---|
| ip route-cache | Controls the use of high-speed switching caches for IP routing. |
| ipv6 cef accounting | Enables CEFv6 and dCEFv6 network accounting. |
| ipv6 cef distributed | Enables distributed CEFv6. |
| show cef | Displays which packets the line cards dropped or displays which packets were not express-forwarded. |
| show ipv6 cef | Displays entries in the IPv6 FIB. |

ipv6 cef accounting

To enable Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) network accounting, use the **ipv6 cef accounting** command in global configuration mode. To disable CEFv6 network accounting, use the **no** form of this command.

```
ipv6 cef accounting [per-prefix] [prefix-length]

no ipv6 cef accounting [per-prefix] [prefix-length]
```

| | | |
|--------------------|---------------|---|
| Syntax Description | per-prefix | (Optional) Enables the collection of the number of packets and bytes express-forwarded to an IPv6 destination (or IPv6 prefix). |
| | prefix-length | (Optional) Enables the collection of the number of packets and bytes express-forwarded to an IPv6 prefix length. |

Defaults CEFv6 network accounting is disabled.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(22)S | This command was introduced. |
| | 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **ipv6 cef accounting** command is similar to the **ip cef accounting** command, except that it is IPv6-specific.

Configuring CEFv6 network accounting enables you to collect statistics on CEFv6 traffic patterns in your network.

When you enable network accounting for CEFv6 by using the **ipv6 cef accounting** command in global configuration mode, accounting information is collected at the Route Processor (RP) when CEFv6 mode is enabled and at the line cards when dCEFv6 mode is enabled. You can then display the collected accounting information using the **show ipv6 cef EXEC** command.

Examples

The following example enables the collection of CEFv6 accounting information globally on the router:

```
ipv6 cef accounting
```

Related Commands

| Command | Description |
|----------------------|---|
| show cef | Displays which packets the line cards dropped or displays which packets were not express-forwarded. |
| show ipv6 cef | Displays entries in the IPv6 FIB. |

ipv6 cef distributed

To enable distributed Cisco Express Forwarding for IPv6 (dCEFv6), use the **ipv6 cef distributed** command in global configuration mode. To disable dCEFv6, use the **no** form of this command.

ipv6 cef distributed

no ipv6 cef distributed

Syntax Description

This command has no arguments or keywords.

Defaults

dCEFv6 is disabled on the Cisco 7500 series routers and enabled on the Cisco 12000 series Internet routers.

Command Modes

Global configuration

Command History

| Release | Modification |
|-----------|---|
| 12.0(22)S | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **ipv6 cef distributed** command is similar to the **ip cef distributed** command, except that it is IPv6-specific.

Enabling dCEFv6 globally on the router by using the **ipv6 cef distributed** in global configuration mode distributes the CEF processing of IPv6 packets from the Route Processor (RP) to the line cards of distributed architecture platforms.



Note

The **ipv6 cef distributed** command is not supported on the Cisco 12000 series Internet routers because dCEFv6 is enabled by default on this platform.



Note

To forward dCEFv6 traffic on the router, configure the forwarding of IPv6 unicast datagrams globally on your router by using the **ipv6 unicast-routing** global configuration command, and configure an IPv6 address and IPv6 processing on an interface by using the **ipv6 address** interface configuration command.



Note

You must enable distributed CEF for IPv4 (dCEFv4) by using the **ip cef distributed** global configuration command before enabling dCEFv6 by using the **ipv6 cef distributed** global configuration command.

CEF is advanced Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with web-based applications and interactive sessions.

Examples

The following example enables dCEFv6 operation:

```
ipv6 cef distributed
```

Related Commands

| Command | Description |
|-----------------------|---|
| ip route-cache | Controls the use of high-speed switching caches for IP routing. |
| show ipv6 cef | Displays entries in the IPv6 FIB. |

ipv6 dhcp client pd

To enable the Dynamic Host Configuration Protocol (DHCP) for IPv6 client process and enable request for prefix delegation through a specified interface, use the **ipv6 dhcp client pd** command in interface configuration mode. To disable requests for prefix delegation, use the **no** form of this command.

ipv6 dhcp client pd *prefix-name* [**rapid-commit**]

no ipv6 dhcp client pd

| | | |
|--------------------|---------------------|---|
| Syntax Description | <i>prefix-name</i> | IPv6 general prefix name. |
| | rapid-commit | (Optional) Allow two-message exchange method for prefix delegation. |

| | |
|----------|--|
| Defaults | Prefix delegation is disabled on an interface. |
|----------|--|

| | |
|---------------|-------------------------|
| Command Modes | Interface configuration |
|---------------|-------------------------|

| | | |
|-----------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 12.3(4)T | This command was introduced. |

| | |
|------------------|--|
| Usage Guidelines | Enabling the ipv6 dhcp client pd command starts the DHCP for IPv6 client process if this process is not yet running. |
| | The ipv6 dhcp client pd command enables request for prefix delegation through the interface on which this command is configured. When prefix delegation is enabled and a prefix is successfully acquired, the prefix is stored in the IPv6 general prefix pool with an internal name defined by the <i>ipv6-prefix</i> argument. Other commands and applications (such as the ipv6 address command) can then refer to the prefixes in the general prefix pool. |
| | The rapid-commit keyword enables the use of the two-message exchange for prefix delegation and other configuration. If it is enabled, the client will include the rapid commit option in a solicit message. |

| | |
|----------|---|
| Examples | The following example enables prefix delegation: ipv6 dhcp client pd dhcp-prefix |
|----------|---|

| | | |
|------------------|---------------------------------|--|
| Related Commands | Command | Description |
| | clear ipv6 dhcp client | Restarts the DHCP for IPv6 client on an interface. |
| | show ipv6 dhcp interface | Displays DHCP for IPv6 interface information. |

ipv6 dhcp database

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent, use the **ipv6 dhcp database** command in global configuration mode. To delete the database agent, use the **no** form of this command.

ipv6 dhcp database *agent-URL* [**write-delay** *seconds*] [**timeout** *seconds*]

no ipv6 dhcp database *agent-URL*

Syntax Description

| | |
|-----------------------------------|--|
| <i>agent-URL</i> | A Flash, NVRAM, FTP, TFTP, or Remote Copy Protocol (RCP) uniform resource locator. |
| write-delay <i>seconds</i> | (Optional) How often (in seconds) DHCP for IPv6 sends database updates. The default is 300 seconds. The minimum write delay is 60 seconds. |
| timeout <i>seconds</i> | (Optional) How long, in seconds, the router waits for a database transfer. |

Defaults

Write-delay default is 300 seconds.
Timeout default is 300 seconds.

Command Modes

Global configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.3(4)T | This command was introduced. |

Usage Guidelines

The **ipv6 dhcp database** command specifies DHCP for IPv6 binding database agent parameters. The user may configure multiple database agents.

The **write-delay** keyword specifies how often, in seconds, that DHCP sends database updates. By default, DHCP for IPv6 server waits 300 seconds before sending any database changes.

The **timeout** keyword specifies how long, in seconds, the router waits for a database transfer. Infinity is defined as 0 seconds, and transfers that exceed the timeout period are aborted. By default, the DHCP for IPv6 server waits 300 seconds before aborting a database transfer. When the system is going to reload, there is no transfer timeout so that the binding table can be stored completely.

Examples

The following example specifies DHCP for IPv6 binding database agent parameters:

```
ipv6 dhcp database tftp://10.0.0.1/dhcp-binding
```

Related Commands

| Command | Description |
|--------------------------------|--|
| show ipv6 dhcp database | Displays DHCP for IPv6 binding database agent information. |

ipv6 dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 server configuration information pool and enter DHCP for IPv6 pool configuration mode, use the **ipv6 dhcp pool** command in global configuration mode. To delete a DHCP for IPv6 pool, use the **no** form of this command.

```
ipv6 dhcp pool poolname

no ipv6 dhcp pool poolname
```

| | | |
|--------------------|----------|--|
| Syntax Description | poolname | User-defined name for the local prefix pool. The pool name can be a symbolic string (such as “Engineering”) or an integer (such as 0). |
|--------------------|----------|--|

| | |
|----------|--|
| Defaults | No DHCP for IPv6 pools are configured. |
|----------|--|

| | |
|---------------|----------------------|
| Command Modes | Global configuration |
|---------------|----------------------|

| | | |
|-----------------|----------|------------------------------|
| Command History | Release | Modification |
| | 12.3(4)T | This command was introduced. |

| | |
|------------------|--|
| Usage Guidelines | Use the ipv6 dhcp pool command to create a DHCP for IPv6 server configuration information pool. When the ipv6 dhcp pool command is enabled, the configuration mode changes to DHCP for IPv6 pool configuration mode. In this mode, the administrator can configure pool parameters, such as prefixes to be delegated and Domain Name System (DNS) servers. Once the DHCP for IPv6 configuration information pool has been created, use the ipv6 dhcp server command to associate the pool with a server on an interface. |
|------------------|--|

| | |
|----------|--|
| Examples | The following example specifies a DHCP for IPv6 configuration information pool named cisco1 and places the router in DHCP for IPv6 pool configuration mode: Router(config)# ipv6 dhcp pool pool1 Router(config-dhcp)# |
|----------|--|

| | | |
|------------------|----------------------------|--|
| Related Commands | Command | Description |
| | ipv6 dhcp server | Enables DHCP for IPv6 service on an interface. |
| | show ipv6 dhcp pool | Displays DHCP for IPv6 configuration pool information. |

ipv6 dhcp server

To enable Dynamic Host Configuration Protocol (DHCP) for IPv6 service on an interface, use the **ipv6 dhcp server** in interface configuration mode. To disable DHCP for IPv6 service on an interface, use the **no** form of this command.

ipv6 dhcp server *poolname* [**rapid-commit**] [**preference value**] [**allow-hint**]

no ipv6 dhcp server

Syntax Description

| | |
|-------------------------|---|
| <i>poolname</i> | User-defined name for the local prefix pool. The pool name can be a symbolic string (such as “Engineering”) or an integer (such as 0). |
| rapid-commit | (Optional) Allow two-message exchange method for prefix delegation. |
| preference value | (Optional) The preference value carried in the preference option in the advertise message sent by the server. The range is from 0 to 255. The preference value defaults to 0. |
| allow-hint | (Optional) Specifies whether the server should consider delegating client suggested prefixes. By default, the server ignores client-hinted prefixes. |

Defaults

DHCP for IPv6 service on an interface is disabled.

Command Modes

Interface configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.3(4)T | This command was introduced. |

Usage Guidelines

The **ipv6 dhcp server** command enables DHCP for IPv6 service on a specified interface using the pool for prefix delegation and other configuration through that interface.

The **rapid-commit** keyword enables the use of the two-message exchange for prefix delegation and other configuration. If a client has included a rapid commit option in the solicit message and the **rapid-commit** keyword is enabled for the server, the server responds to the solicit message with a reply message.

If the **preference** keyword is configured with a value other than 0, the server adds a preference option to carry the preference value for the advertise messages. This action affects the selection of a server by the client. Any advertise message that does not include a preference option is considered to have a preference value of 0. If the client receives an advertise message that includes a preference option with a preference value of 255, the client immediately sends a request message to the server from which the advertise message was received.

If the **allow-hint** keyword is specified, the server will delegate a valid client-suggested prefix in the solicit and request messages. The prefix is valid if it is in the associated local prefix pool and it is not assigned to a device. If the **allow-hint** keyword is not specified, a hint is ignored and a prefix is delegated from the free list in the pool.

Examples

The following example enables DHCP for IPv6 for the local prefix pool named server1.

```
ipv6 dhcp server dhcp-pool
```

Related Commands

| Command | Description |
|--------------------------|---|
| ipv6 dhcp pool | Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode. |
| show ipv6 dhcp interface | Displays DHCP for IPv6 interface information. |

ipv6 enable

To enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **ipv6 enable** command in interface configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

ipv6 enable

no ipv6 enable

Syntax Description

This command has no arguments or keywords.

Defaults

IPv6 is disabled.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **ipv6 enable** command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing. The **no ipv6 enable** command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Examples

The following example enables IPv6 processing on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 enable
```

Related Commands

| Command | Description |
|--------------------------------|--|
| ipv6 address link-local | Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface. |
| ipv6 address eui-64 | Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address. |
| ipv6 unnumbered | Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface. |
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 general-prefix

To define an IPv6 general prefix, use the **ipv6 general-prefix** command in global configuration mode. To remove the IPv6 general prefix, use the **no** form of this command.

```

ipv6 general-prefix prefix-name {ipv6-prefix/prefix-length | 6to4 interface-type interface-number}

no ipv6 general-prefix prefix-name
  
```

Syntax Description

| | |
|--|--|
| <i>prefix-name</i> | The name assigned to the prefix. |
| <i>ipv6-prefix</i> | <p>The IPv6 network assigned to the general prefix.</p> <p>This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</p> <p>When defining a general prefix manually, specify both the <i>ipv6-prefix</i> and <i>lprefix-length</i> arguments.</p> |
| <i>lprefix-length</i> | <p>The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.</p> <p>When defining a general prefix manually, specify both the <i>ipv6-prefix</i> and <i>lprefix-length</i> arguments.</p> |
| 6to4 | <p>Allows configuration of a general prefix based on an interface used for 6to4 tunneling.</p> <p>When defining a general prefix based on a 6to4 interface, specify the 6to4 keyword and the <i>interface-type interface-number</i> argument.</p> |
| <i>interface-type</i> <i>interface-number</i> | <p>Interface type and number. For more information, use the question mark (?) online help function.</p> <p>When defining a general prefix based on a 6to4 interface, specify the 6to4 keyword and the <i>interface-type interface-number</i> argument.</p> |

Defaults

No general prefix is defined.

Command Modes

Global configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.3(4)T | This command was introduced. |

Usage Guidelines

Use the **ipv6 general-prefix** command to define an IPv6 general prefix.

A general prefix holds a short prefix, based on which a number of longer, more specific, prefixes can be defined. When the general prefix is changed, all of the more specific prefixes based on it will change, too. This function greatly simplifies network renumbering and allows for automated prefix definition.

More specific prefixes, based on a general prefix, can be used when configuring IPv6 on an interface. When defining a general prefix based on an interface used for 6to4 tunneling, the general prefix will be of the form 2002:a.b.c.d::/48, where “a.b.c.d” is the IPv4 address of the interface referenced.

Examples

The following example manually defines an IPv6 general prefix named my-prefix:

```
Router(config)# ipv6 general-prefix my-prefix 2001:DB8:2222::/48
```

The following example defines an IPv6 general prefix named my-prefix based on a 6to4 interface:

```
Router(config)# ipv6 general-prefix my-prefix 6to4 ethernet0
```

Related Commands

| Command | Description |
|---------------------------------|---|
| show ipv6 general-prefix | Displays information on general prefixes for an IPv6 addresses. |

ipv6 hop-limit

To configure the maximum number of hops used in router advertisements and all IPv6 packets that are originated by the router, use the **ipv6 hop-limit** command in global configuration mode. To return the hop limit to its default value, use the **no** form of this command.

```
ipv6 hop-limit value
no ipv6 hop-limit value
```

| | | |
|--------------------|-------|--|
| Syntax Description | value | The maximum number of hops. The acceptable range is from 1 to 255. |
|--------------------|-------|--|

| | |
|----------|---------|
| Defaults | 64 hops |
|----------|---------|

| | |
|---------------|----------------------|
| Command Modes | Global configuration |
|---------------|----------------------|

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

| | |
|----------|--|
| Examples | <p>The following example configures a maximum number of 15 hops for router advertisements and all IPv6 packets that are originated from the router:</p> <pre>Router(config)# ipv6 hop-limit 15</pre> |
|----------|--|

ipv6 host

To define a static host name-to-address mapping in the host name cache, use the **ipv6 host** command in global configuration mode. To remove the host name-to-address mapping, use the **no** form of this command.

ipv6 host *name* [*port*] *ipv6-address1* [*ipv6-address2...ipv6-address4*]

no ipv6 host *name*

Syntax Description

| | |
|--------------------------------------|--|
| <i>name</i> | Name of the IPv6 host. The first character can be either a letter or a number. If you use a number, the operations you can perform are limited. |
| <i>port</i> | (Optional) The default Telnet port number for the associated IPv6 addresses. |
| <i>ipv6-address1</i> | Associated IPv6 address. 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>ipv6-address2...ipv6-address4</i> | (Optional) Additional associated IPv6 addresses. You can bind up to four addresses to a host name. |

Defaults

Static host name-to-address mapping in the host name cache is not defined.
The default Telnet port is 23.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **ipv6 host** command is similar to the **ip host** command, except that it is IPv6-specific.
The first character of the name can be either a letter or a number. If you use a number, the operations you can perform (such as **ping**) are limited.

Examples

The following example defines two static mappings:

```
Router(config)# ipv6 host cisco-sj 2001:0DB8:1::12
Router(config)# ipv6 host cisco-hq 2002:C01F:768::1 2001:0DB8:1::12
```

Related Commands

| Command | Description |
|------------|---|
| show hosts | Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses. |

ipv6 icmp error-interval

To configure the interval and bucket size for IPv6 Internet Control Message Protocol (ICMP) error messages, use the **ipv6 icmp error-interval** command in global configuration mode. To return the interval to its default setting, use the **no** form of this command.

ipv6 icmp error-interval *milliseconds* [*bucketsize*]

no ipv6 icmp error-interval

Syntax Description

| | |
|---------------------|---|
| <i>milliseconds</i> | The time interval between tokens being placed in the bucket. The acceptable range is from 0 to 2147483647 with a default of 100 milliseconds. |
| <i>bucketsize</i> | (Optional) The maximum number of tokens stored in the bucket. The acceptable range is from 1 to 200 with a default of 10 tokens. |

Defaults

ICMP rate limiting is enabled by default. To disable ICMP rate limiting, set the interval to zero.

100 milliseconds

10 tokens

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.2(8)T | Support for IPv6 ICMP rate limiting was extended to use token buckets. |
| 12.0(21)ST | This command, without the extension to use token buckets, was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command, without the extension to use token buckets, was integrated into Cisco IOS Release 12.0(22)S. |
| 12.0(23)S | This command, with the support for IPv6 ICMP rate limiting extended to use token buckets, was integrated into Cisco IOS Release 12.0(23)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

Use the **ipv6 icmp error-interval** global configuration command to limit the rate at which IPv6 ICMP error messages are sent. A token bucket algorithm is used with one token representing one IPv6 ICMP error message. Tokens are placed in the virtual bucket at a specified interval until the maximum number of tokens allowed in the bucket is reached.

The *milliseconds* argument specifies the time interval between tokens arriving in the bucket. The optional *bucketsize* argument is used to define the maximum number of tokens allowed in the bucket. Tokens are removed from the bucket when IPv6 ICMP error messages are sent, which means that if the *bucketsize* is set to 20, a rapid succession of 20 IPv6 ICMP error messages can be sent. When the bucket is empty of tokens, IPv6 ICMP error messages are not sent until a new token is placed in the bucket.

Use the **show ipv6 traffic EXEC** command to display IPv6 ICMP rate-limited counters.

Examples

The following example shows an interval of 50 milliseconds and a bucket size of 20 tokens being configured for IPv6 ICMP error messages:

```
ipv6 icmp error-interval 50 20
```

Related Commands

| Command | Description |
|-------------------|---|
| show ipv6 traffic | Displays statistics about IPv6 traffic. |

ipv6 local pool

To configure a local IPv6 prefix pool, use the **ipv6 local pool** configuration command with the prefix pool name. To disband the pool, use the **no** form of this command.

ipv6 local pool *poolname* *prefix/prefix-length* *assigned-length* [**shared**] [**cache-size** *size*]

no ipv6 local pool *poolname*

| Syntax Description | |
|-------------------------------|--|
| <i>poolname</i> | User-defined name for the local prefix pool. |
| <i>prefix</i> | IPv6 prefix assigned to the pool. 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> | The length of the IPv6 prefix assigned to the pool. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). |
| <i>assigned-length</i> | Length of prefix, in bits, assigned to the user from the pool. The value of the <i>assigned-length</i> argument cannot be less than the value of the <i>/prefix-length</i> argument. |
| shared | (Optional) Indicates that the pool is a shared pool. |
| cache-size <i>size</i> | (Optional) Specifies the size of the cache. |

Defaults No pool is configured.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 12.2(13)T | This command was introduced. |

Usage Guidelines

- All pool names must be unique.
- IPv6 prefix pools have a function similar to IPv4 address pools. Contrary to IPv4, a block of addresses (an address prefix) are assigned and not single addresses.
- Prefix pools are not allowed to overlap.
- Once a pool is configured, it cannot be changed. To change the configuration, the pool must be removed and recreated. All prefixes already allocated will also be freed.

Examples

This example shows the creation of an IPv6 prefix pool.

```
Router (config)# ipv6 local pool pool1 2001:0DB8::/29 64
Router# show ipv6 local pool
```

```
Pool Prefix Free In use
pool1 2001:0DB8::/29 65516 20
```

Related Commands

| Command | Description |
|---------------------------------------|--|
| debug ipv6 pool | Enables IPv6 pool debugging. |
| peer default ipv6 address pool | Specifies the pool from which client prefixes are assigned for PPP links. |
| prefix-delegation pool | Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients. |
| show ipv6 local pool | Displays information about any defined IPv6 address pools. |

ipv6 mfib

To reenable IPv6 multicast forwarding on the router, use the **ipv6 mfib** command in global configuration mode. To disable IPv6 multicast forwarding on the router, use the **no** form of this command.

ipv6 mfib

no ipv6 mfib

Syntax Description

The command has no arguments or keywords.

Defaults

Multicast forwarding is enabled automatically when IPv6 multicast routing is enabled.

Command Modes

Global configuration

Command History

| Release | Modification |
|-----------|---|
| 12.3(2)T | This command was introduced. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

After a user has enabled the **ipv6 multicast-routing** command, IPv6 multicast forwarding is enabled. Because IPv6 multicast forwarding is enabled by default, use the **no** form of the **ipv6 mfib** command to disable IPv6 multicast forwarding.

Examples

The following example disables multicast forwarding on the router:

```
no ipv6 mfib
```

Related Commands

| Command | Description |
|-------------------------------|--|
| ipv6 multicast-routing | Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding. |

ipv6 mfib fast

To enable Multicast Forwarding Information Base (MFIB) interrupt-level IPv6 multicast forwarding of outgoing packets on a specific interface, use the **ipv6 mfib fast** command in interface configuration mode. To disable MFIB interrupt-level IPv6 multicast forwarding, use the **no** form of this command.

ipv6 mfib fast

no ipv6 mfib fast

Syntax Description

This command has no arguments or keywords.

Defaults

Cisco Express Forwarding (CEF)-based forwarding is enabled by default on interfaces that support it.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-----------|---|
| 12.3(2)T | This command was introduced. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

After a user has enabled the **ipv6 multicast-routing** command, MFIB interrupt switching is enabled to run on every interface. Use the **no** form of the **ipv6 mfib fast** command to disable interrupt-switching on a specific interface.

Use the **show ipv6 mfib interface** command to display the multicast forwarding status of interfaces.

Examples

The following example disables MFIB interrupt switching on Fast Ethernet interface 1/0:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# no ipv6 mfib fast
```

Related Commands

| Command | Description |
|---------------------------------|--|
| ipv6 multicast-routing | Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding. |
| show ipv6 mfib interface | Displays IPv6 multicast-enabled interfaces and their forwarding status. |

ipv6 mfib-mode centralized-only

To reenables distributed forwarding, use the **ipv6 mfib-mode centralized-only** command in global configuration mode. To reenables multicast forwarding, use the **no** form of this command.

ipv6 mfib-mode centralized-only

no ipv6 mfib-mode centralized-only

Syntax Description This command has no arguments or keywords.

Defaults Multicast distributed forwarding is enabled.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-----------|--|
| | 12.0(26)S | This command was introduced. |
| | 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |
| | | |

Usage Guidelines The **ipv6 mfib-mode centralized-only** command is available only on distributed platforms. Distributed forwarding is enabled by default when the **ipv6 multicast-routing**, **ipv6 cef distributed**, and the **ipv6 mfib** commands are enabled. The **ipv6 mfib-mode centralized-only** command reenables distributed forwarding. All multicast forwarding is performed centrally.

Examples The following example reenables distributed forwarding:

```

ipv6 mfib-mode centralized-only

```

ipv6 mld access-group

To perform IPv6 multicast receiver access control, use the **ipv6 mld access-group** command in interface configuration mode. To stop using multicast receiver access control, use the **no** form of this command.

```
ipv6 mld access-group access-list-name

no ipv6 mld access-group access-list-name
```

| | | |
|--------------------|------------------|---|
| Syntax Description | access-list-name | A standard IPv6 named access list that defines the multicast groups and sources to allow or deny. |
|--------------------|------------------|---|

| | |
|----------|-------------------------------------|
| Defaults | All groups and sources are allowed. |
|----------|-------------------------------------|

| | |
|---------------|-------------------------|
| Command Modes | Interface configuration |
|---------------|-------------------------|

| | | |
|-----------------|-----------|--|
| Command History | Release | Modification |
| | 12.0(26)S | This command was introduced. |
| | 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

The **ipv6 mld access-group** command is used for receiver access control and to check the groups and sources in Multicast Listener Discovery (MLD) reports against the access list. The **ipv6 mld access-group** command also limits the state created by MLD reports. Because Cisco supports MLD version 2, the **ipv6 mld access-group** command allows users to limit the list of groups a receiver can join. You can also use this command to allow or deny sources used to join Source Specific Multicast (SSM) channels.

If a report (S1, S2...Sn, G) is received, the group (0, G) is first checked against the access list. If the group is denied, the entire report is denied. If the report is allowed, each individual (Si, G) is checked against the access list. State is not created for the denied sources.

Examples

The following example creates an access list called acc-grp-1 and denies all the state for group ff04::10:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# deny ipv6 any host ff04::10
Router(config-ipv6-acl)# permit ipv6 any any
Router(config-ipv6-acl)# interface ethernet 0/0
Router(config-if)# ipv6 mld access-group acc-grp-1
```

The following example creates an access list called acc-grp-1 and permits all the state for only group ff04::10:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 any host ff04::10
Router(config-ipv6-acl)# interface ethernet 0/0
Router(config-if)# ipv6 mld access-group acc-grp-1
```

The following example permits only EXCLUDE(G,{ }) reports. This example converts EXCLUDE(G,{S1, S2..Sn}) into EXCLUDE(G,{ }):

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 host :: host ff04::10
Router(config-ipv6-acl)# deny ipv6 any host ff04::10
Router(config-ipv6-acl)# permit ipv6 any any
Router(config-ipv6-acl)# interface ethernet 0/0
Router(config-if)# ipv6 mld access-group acc-grp-1
```

The following example filters a particular source 100::1 for a group ff04::10:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# deny ipv6 host 100::1 host ff04::10
Router(config-ipv6-acl)# permit ipv6 any host ff04::10
Router(config-ipv6-acl)# interface ethernet 0/0
Router(config-if)# ipv6 mld access-group acc-grp-1
```

ipv6 mld join-group

To configure Multicast Listener Discovery (MLD) reporting for a specified group and source, use the **ipv6 mld join-group** command in interface configuration mode. To cancel reporting and leave the group, use the **no** form of this command.

ipv6 mld join-group [*group-name* | *group-address*] [[**include** | **exclude**] *source-address* | *source-name*]

no ipv6 mld join-group [*group-name* | *group-address*] [[**include** | **exclude**] *source-address* | *source-name*]

Syntax Description

| | |
|--|--|
| <i>group-name</i> <i>group-address</i> | (Optional) IPv6 address or name of the multicast group. |
| include | (Optional) Enables include mode. |
| exclude | (Optional) Enables exclude mode. |
| <i>source-address</i> <i>source-name</i> | (Optional) Unicast source address or name to include or exclude. |

Defaults

If a source is specified and no mode is specified, the default is to include the source.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-----------|---|
| 12.3(2)T | This command was introduced. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

The **ipv6 mld join-group** command configures MLD reporting for a specified source and group. The packets that are addressed to a specified group address will be passed up to the client process in the router. The packets will be forwarded out the interface depending on the normal Protocol Independent Multicast (PIM) activity.

If the **ipv6 mld join-group** command is repeated for the same group, only the most recent command will take effect. For example, if you enter the following commands, only the second command is saved and will appear in the MLD cache:

```
Router(config-if)ipv6 mld join-group ff05::10 include 2000::1
Router(config-if)ipv6 mld join-group ff05::10 include 2000::2
```

Examples

The following example configures MLD reporting for specific groups:

```
ipv6 mld join-group ff04::10
```

Related Commands

| Command | Description |
|---------------------------|---|
| no ipv6 mld router | Disables MLD router-side processing on a specified interface. |

ipv6 mld query-interval

To configure the frequency at which the Cisco IOS software sends Multicast Listener Discovery (MLD) host-query messages, use the **ipv6 mld query-interval** command in interface configuration mode. To return to the default frequency, use the **no** form of this command.

ipv6 mld query-interval *seconds*

no ipv6 mld query-interval

| | | |
|--------------------|----------------|--|
| Syntax Description | <i>seconds</i> | Frequency, in seconds, at which to send MLD host-query messages. It can be a number from 0 to 65535. The default is 125 seconds. |
|--------------------|----------------|--|

| | |
|----------|------------------------------|
| Defaults | <i>seconds</i> : 125 seconds |
|----------|------------------------------|

| | |
|---------------|-------------------------|
| Command Modes | Interface configuration |
|---------------|-------------------------|

| Command History | <table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.3(2)T</td><td>This command was introduced.</td></tr><tr><td>12.2(18)S</td><td>This command was integrated into Cisco IOS Release 12.2(18)S.</td></tr><tr><td>12.0(26)S</td><td>This command was integrated into Cisco IOS Release 12.0(26)S.</td></tr></table> | Release | Modification | 12.3(2)T | This command was introduced. | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |
|-----------------|--|---------|--------------|----------|------------------------------|-----------|---|-----------|---|
| Release | Modification | | | | | | | | |
| 12.3(2)T | This command was introduced. | | | | | | | | |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. | | | | | | | | |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. | | | | | | | | |


Usage Guidelines

Multicast routers send host membership query messages (host-query messages) to discover which multicast groups have members on the router’s attached networks. Hosts respond with MLD report messages indicating that they want to receive multicast packets for specific groups (that is, indicating that the host wants to become a member of the group).

The designated router for a LAN is the only router that sends MLD host-query messages.

The query interval is calculated as $\text{query interval} = (2 \times \text{query interval}) + \text{query-max-response-time} / 2$. If the **ipv6 mld query-interval** command is configured to be 60 seconds and the **ipv6 mld query-max-response-time** command is configured to be 20 seconds, then the **ipv6 mld query-timeout command** should be configured to be 130 seconds or higher.

This command works with the **ipv6 mld query-max-response-time** and **ipv6 mld query-timeout** commands. If you change the default value for the **ipv6 mld query-interval** command, make sure the changed value works correctly with these two commands.


Caution

Changing the default value may severely impact multicast forwarding.

Examples

The following example sets the MLD query interval to 60 seconds:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 mld query-interval 60
```

Related Commands

| Command | Description |
|---|--|
| ipv6 mld query-max-response-time | Configures the maximum response time advertised in MLD queries. |
| ipv6 mld query-timeout | Configures the timeout value before the router takes over as the querier for the interface. |
| ipv6 pim hello-interval | Configures the frequency of PIM hello messages on an interface. |
| show ipv6 mld groups | Displays the multicast groups that are directly connected to the router and that were learned through MLD. |

ipv6 mld query-max-response-time

To configure the maximum response time advertised in Multicast Listener Discovery (MLD) queries, use the **ipv6 mld query-max-response-time** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 mld query-max-response-time *seconds*

no ipv6 mld query-max-response-time

| | | |
|--------------------|----------------|--|
| Syntax Description | <i>seconds</i> | Maximum response time, in seconds, advertised in MLD queries. The default value is 10 seconds. |
|--------------------|----------------|--|

| | |
|----------|-----------------------------|
| Defaults | <i>seconds</i> : 10 seconds |
|----------|-----------------------------|

| | |
|---------------|-------------------------|
| Command Modes | Interface configuration |
|---------------|-------------------------|

| | | |
|-----------------|-----------|---|
| Command History | Release | Modification |
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

| | |
|------------------|--|
| Usage Guidelines | This command controls how much time the hosts have to answer an MLD query message before the router deletes their group. Configuring a value of fewer than 10 seconds enables the router to prune groups faster. |
|------------------|--|



Note

If the hosts do not respond fast enough, they might be pruned inadvertently. Therefore, the hosts must know to respond faster than 10 seconds (or the value you configure).

The query interval is calculated as $\text{query interval} = (2 \times \text{query interval}) + \text{query-max-response-time} / 2$. If the **ipv6 mld query-interval** command is configured to be 60 seconds and the **ipv6 mld query-max-response-time** command is configured to be 20 seconds, then the **ipv6 mld query-timeout command** should be configured to be 130 seconds or higher.

This command works with the **ipv6 mld query-interval** and **ipv6 mld query-timeout** commands. If you change the default value for the **ipv6 mld query-max-response-time** command, make sure the changed value works correctly with these two commands.



Caution

Changing the default value may severely impact multicast forwarding.

| | |
|----------|---|
| Examples | The following example configures a maximum response time of 20 seconds: |
|----------|---|


```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 mld query-max-response-time 20
```

| Related Commands | Command | Description |
|------------------|--------------------------------|--|
| | ipv6 mld query-interval | Configures the frequency at which the Cisco IOS software sends MLD host-query messages. |
| | ipv6 mld query-timeout | Configures the timeout value before the router takes over as the querier for the interface. |
| | ipv6 pim hello-interval | Configures the frequency of PIM hello messages on an interface. |
| | show ipv6 mld groups | Displays the multicast groups that are directly connected to the router and that were learned through MLD. |

ipv6 mld query-timeout

To configure the timeout value before the router takes over as the querier for the interface, use the **ipv6 mld query-timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 mld query-timeout *seconds*

no ipv6 mld query-timeout

| | | |
|---------------------------|----------------|--|
| Syntax Description | <i>seconds</i> | Number of seconds that the router waits after the previous querier has stopped querying and before it takes over as the querier. |
|---------------------------|----------------|--|

| | |
|-----------------|------------------------------|
| Defaults | <i>seconds</i> : 250 seconds |
|-----------------|------------------------------|

| | |
|----------------------|-------------------------|
| Command Modes | Interface configuration |
|----------------------|-------------------------|

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

The query interval is calculated as $\text{query interval} = (2 \times \text{query interval}) + \text{query-max-response-time} / 2$. If the **ipv6 mld query-interval** command is configured to be 60 seconds and the **ipv6 mld query-max-response-time** command is configured to be 20 seconds, then the **ipv6 mld query-timeout** command should be configured to be 130 seconds or higher.

This command works with the **ipv6 mld query-interval** and **ipv6 mld query-max-response-time** commands. If you change the default value for the **ipv6 mld query-timeout** command, make sure the changed value works correctly with these two commands.



Caution

Changing the default value may severely impact multicast forwarding.

Examples

The following example configures the router to wait 130 seconds from the time it received the last query before it takes over as the querier for the interface:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 mld query-timeout 130
```

| Related Commands | Command | Description |
|------------------|---|---|
| | ipv6 mld query-interval | Configures the frequency at which the Cisco IOS software sends MLD host-query messages. |
| | ipv6 mld query-max-response-time | Configures the maximum response time advertised in MLD queries. |

ipv6 mld router

To enable Multicast Listener Discovery (MLD) router-side processing on a specified interface, use the **ipv6 mld router** command in interface configuration mode. To disable MLD router-side processing on a specified interface, use the **no** form of the command.

ipv6 mld router

no ipv6 mld router

Syntax Description This command has no arguments or keywords.

Defaults MLD is enabled on the interface.

Command Modes Interface configuration

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines When the **ipv6 multicast-routing** command is configured, MLD router-side processing is enabled on every interface. The **no ipv6 mld router** command disables MLD router-side processing on a specified interface. When MLD router-side processing is disabled, the router stops sending MLD queries and stops keeping track of MLD members on the LAN.

If the **ipv6 mld join-group** command is also configured on an interface, it will continue with MLD host functionality and will report group membership when an MLD query is received.

MLD host-side processing is enabled by default. The **ipv6 multicast-routing** command does not enable or disable MLD host-side processing.

Examples The following example disables MLD router-side processing on an interface:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# no ipv6 mld router
```

| Related Commands | Command | Description |
|------------------|-------------------------------|--|
| | ipv6 mld join-group | Configures MLD reporting for a specified group and source. |
| | ipv6 multicast-routing | Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding. |

ipv6 mld static-group

To statically forward traffic for the multicast group onto a specified interface and cause the interface to behave as if a Multicast Listener Discovery (MLD) joiner were present on the interface, use the **ipv6 mld static-group** command in interface configuration mode. To stop statically forwarding traffic for the specific multicast group, use the **no** form of this command.

```

ipv6 mld static-group [group-name | group-address] [[include | exclude] source-address |
source-name]
  
```

```

no ipv6 mld static-group [group-name | group-address] [[include | exclude] source-address |
source-name]
  
```

Syntax Description

| | |
|---|--|
| <i>group-name</i> <i>group-address</i> | (Optional) IPv6 address or name of the multicast group. |
| include | (Optional) Enables include mode. |
| exclude | (Optional) Enables exclude mode. |
| source-address source-name | (Optional) Unicast source address or name to include or exclude. |

Defaults

If no mode is specified for the source, use of the **include** keyword is the default.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-----------|---|
| 12.3(2)T | This command was introduced. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

The **ipv6 multicast-routing** command must be configured for the **ipv6 mld static-group** command to be effective.

When the **ipv6 mld static-group** command is enabled, packets to the group are either fast-switched or hardware-switched, depending on the platform. Unlike what happens when using the **ipv6 mld join-group** command, a copy of the packet is not sent to the process level.



Note

Using the **ipv6 mld static-group** command is not sufficient to allow traffic to be forwarded onto the interface. Other conditions, such as the absence of a route, the router not being the designated router, or losing an assert, can cause the router not to forward traffic even if the **ipv6 mld static-group** command is configured.

Examples

The following example statically forward traffic for the multicast group onto the specified interface:

```
ipv6 mld static-group ff04::10 include 100::1
```

Related Commands

| Command | Description |
|-------------------------------|--|
| ipv6 mld join-group | Configures MLD reporting for a specified group and source. |
| no ipv6 mld router | Disables MLD router-side processing on a specified interface. |
| ipv6 multicast-routing | Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding. |
| no ipv6 pim | Use the no form of the ipv6 pim command to disable PIM on a specified interface. |

ipv6 mtu

To set the maximum transmission unit (MTU) size of IPv6 packets sent on an interface, use the **ipv6 mtu** command in interface configuration mode. To restore the default MTU size, use the **no** form of this command.

ipv6 mtu *bytes*

no ipv6 mtu *bytes*

Syntax Description

| | |
|-------|-----------------|
| bytes | MTU (in bytes). |
|-------|-----------------|

Defaults

The default value depends on the interface medium, but the minimum for any interface is 1280 bytes.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

If a nondefault value is configured for an interface, an MTU option is included in router advertisements. IPv6 routers do not fragment forwarded IPv6 packets. Traffic originating from IPv6 routers may be fragmented.

All devices on a physical medium must have the same protocol MTU in order to operate.

In addition to the “IPv6 MTU value” (set by using the **ipv6 mtu** command), interfaces also have a nonprotocol specific “MTU value,” which is set by using the **mtu** interface configuration command.



Note

The “MTU value” configured by using the **mtu** interface configuration command must not be less than 1280 bytes.

Examples

The following example sets the maximum IPv6 packet size for serial interface 0/1 to 2000 bytes:

```
Router(config)# interface serial 0/1
Router(config-if)# ipv6 mtu 2000
```

Related Commands

| Command | Description |
|----------------------------|--|
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 multicast-routing

To enable multicast routing using Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD) on all IPv6-enabled interfaces of the router and to enable multicast forwarding, use the **ipv6 multicast-routing** command in global configuration mode. To stop multicast routing and forwarding, use the **no** form of this command.

ipv6 multicast-routing

no ipv6 multicast-routing

Syntax Description This command has no arguments or keywords.

Defaults Multicast routing is not enabled.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines Enabling IPv6 multicast on all interfaces also includes enabling PIM and MLD protocol processing on the interfaces. Users may configure specific interfaces before multicast is enabled, so that they can then disable PIM and MLD protocol processing on interfaces, as needed.

Examples The following example enables multicast routing and turns on PIM and MLD on all interfaces:

```
ipv6 multicast-routing
```

| Related Commands | Command | Description |
|------------------|----------------------------|--|
| | ipv6 pim rp-address | Configures the address of a PIM RP for a particular group range. |
| | no ipv6 pim | Turns off IPv6 PIM on a specified interface. |
| | no ipv6 mld router | Disables MLD router-side processing on a specified interface. |

ipv6 nat

To designate that traffic originating from or destined for the interface is subject to Network Address Translation - Protocol Translation (NAT-PT), use the **ipv6 nat** command in interface configuration mode. To prevent the interface from being able to translate, use the **no** form of this command.

ipv6 nat

no ipv6 nat

Syntax Description

This command has no keywords or arguments.

Defaults

Traffic leaving or arriving at this interface is not subject to NAT-PT.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-----------|------------------------------|
| 12.2(13)T | This command was introduced. |

Usage Guidelines

The **ipv6 nat** command is usually specified on at least one IPv4 interface and one IPv6 interface at the networking device where you intend to use NAT-PT.

Examples

The following example assigns the IPv4 address 192.168.30.1 to Fast Ethernet interface 1/0 and the IPv6 address 2001:0DB8:0:1::1 to Fast Ethernet interface 2/0. IPv6 routing is globally enabled and both interfaces are configured to run IPv6 and enable NAT-PT translations.

```
interface fastethernet 1/0
 ip address 192.168.30.1 255.255.255.0
 ipv6 nat
!
interface fastethernet 2/0
 ipv6 address 2001:0DB8:0:1::1/64
 ipv6 nat
```

Related Commands

| Command | Description |
|-----------------------------------|---|
| ipv6 address link-local | Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface. |
| ipv6 address eui-64 | Configures an IPv6 address for an interface and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address. |
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |
| show ipv6 nat translations | Displays active NAT-PT translations. |

ipv6 nat max-entries

To specify the maximum number of Network Address Translation - Protocol Translation (NAT-PT) translation entries stored by the router, use the **ipv6 nat max-entries** command in global configuration mode. To restore the default number of NAT-PT entries, use the **no** form of this command.

ipv6 nat max-entries *number*

no ipv6 nat max-entries

| | | |
|--------------------|---------------|---|
| Syntax Description | <i>number</i> | (Optional) Specifies the maximum number (1–2147483647) of NAT-PT translation entries. Default is unlimited. |
|--------------------|---------------|---|

| | | |
|----------|-------------------------------------|--|
| Defaults | Unlimited number of NAT-PT entries. | |
|----------|-------------------------------------|--|

| | | |
|---------------|----------------------|--|
| Command Modes | Global configuration | |
|---------------|----------------------|--|

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 12.2(13)T | This command was introduced. |

| | | |
|------------------|--|--|
| Usage Guidelines | Use the ipv6 nat max-entries command to set the maximum number of NAT-PT translation entries stored by the router when the router memory is limited, or the actual number of translations is important. | |
|------------------|--|--|

| | | |
|----------|---|--|
| Examples | The following example sets the maximum number of NAT-PT translation entries to 1000: ip nat max-entries 1000 | |
|----------|---|--|

| Related Commands | Command | Description |
|------------------|-----------------------------------|--|
| | clear ipv6 nat translation | Clears dynamic NAT-PT translations from the translation table. |
| | show ipv6 nat translations | Displays active NAT-PT translations. |

ipv6 nat prefix

To assign an IPv6 prefix where matching IPv6 packets will be translated using Network Address Translation - Protocol Translation (NAT-PT), use the **ipv6 nat prefix** command in global configuration or interface configuration mode. To prevent the IPv6 prefix from being used by NAT-PT, use the **no** form of this command.

ipv6 nat prefix *ipv6-prefix/prefix-length*

no ipv6 nat prefix *ipv6-prefix/prefix-length*

| | | |
|--------------------|-----------------------|--|
| Syntax Description | <i>ipv6-prefix</i> | The IPv6 network used as the NAT-PT prefix. 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> | The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). The only prefix length supported is 96. A slash mark must precede the decimal value. |

Defaults No IPv6 prefixes are used by NAT-PT.

Command Modes Global configuration
Interface configuration

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 12.2(13)T | This command was introduced. |

Usage Guidelines The **ipv6 nat prefix** command is used to specify an IPv6 address prefix against which the destination prefix in an IPv6 packet is matched. If the match is successful, NAT-PT will translate the IPv6 packet to an IPv4 packet using the configured mapping rules.

Use the **ipv6 nat prefix** command in global configuration mode to assign a global NAT-PT NAT-PT prefix, or in interface configuration mode to assign a different NAT-PT prefix for each interface. Using a different NAT-PT prefix on several interfaces allows the NAT-PT router to support an IPv6 network with multiple exit points to IPv4 networks.

Examples The following example assigns the IPv6 prefix 2001:0DB8:1::/96 as the global NAT-PT prefix:

```
ipv6 nat prefix 2001:0DB8:1::/96
```

The following example assigns the IPv6 prefix 2001:0DB8:2::/96 as the NAT-PT prefix for the Fast Ethernet interface 1/0, and the IPv6 prefix 2001:0DB8:4::/96 as the NAT-PT prefix for the Fast Ethernet interface 2/0:

```
interface fastethernet 1/0
```

```

ipv6 address 2001:0DB8:2:1::1/64
ipv6 nat prefix 2001:0DB8:2::/96
!
interface fastethernet 2/0
ipv6 address 2001:0DB8:4:1::1/64
ipv6 nat prefix 2001:0DB8:4::/96

```

Related Commands

| Command | Description |
|-----------------------------------|---|
| ipv6 address link-local | Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface. |
| ipv6 address eui-64 | Configures an IPv6 address for an interface and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address. |
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |
| show ipv6 nat translations | Displays active NAT-PT translations. |

ipv6 nat translation

To change the amount of time after which Network Address Translation - Protocol Translation (NAT-PT) translations time out, use the **ipv6 nat translation** command in global configuration mode. To disable the timeout, use the **no** form of this command.

ipv6 nat translation { **timeout** | **udp-timeout** | **dns-timeout** | **tcp-timeout** | **finrst-timeout** | **icmp-timeout** | **syn-timeout** } { *seconds* | **never** }

no ipv6 nat translation { **timeout** | **udp-timeout** | **dns-timeout** | **tcp-timeout** | **finrst-timeout** | **icmp-timeout** | **syn-timeout** }

| Syntax Description | | |
|-----------------------|--|---|
| timeout | | Specifies that the timeout value applies to dynamic translations. Default is 86400 seconds (24 hours). |
| udp-timeout | | Specifies that the timeout value applies to the User Datagram Protocol (UDP) port. Default is 300 seconds (5 minutes). |
| dns-timeout | | Specifies that the timeout value applies to connections to the Domain Naming System (DNS). Default is 60 seconds. |
| tcp-timeout | | Specifies that the timeout value applies to the TCP port. Default is 86400 seconds (24 hours). |
| finrst-timeout | | Specifies that the timeout value applies to Finish and Reset TCP packets, which terminate a connection. Default is 60 seconds. |
| icmp-timeout | | Specifies the timeout value for Internet Control Message Protocol (ICMP) flows. Default is 60 seconds. |
| syn-timeout | | Specifies that the timeout value applies when a TCP SYN (request to synchronize sequence numbers used when opening a connection) flag is received but the flag is not followed by data belonging to the same TCP session. |
| <i>seconds</i> | | Number of seconds after which the specified translation timer expires. The default is 0. |
| never | | Specifies that the dynamic translation timer never expires. |

| Defaults | |
|------------------------|--------------------------|
| timeout: | 86400 seconds (24 hours) |
| udp-timeout: | 300 seconds (5 minutes) |
| dns-timeout: | 60 seconds (1 minute) |
| tcp-timeout: | 86400 seconds (24 hours) |
| finrst-timeout: | 60 seconds (1 minute) |
| icmp-timeout: | 60 seconds (1 minute) |

| Command Modes | |
|---------------|----------------------|
| | Global configuration |

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 12.2(13)T | This command was introduced. |

Usage Guidelines

Dynamic translations time out after a period of time without any translations. The default timeout period is 24 hours. When port translation is configured, there is finer control over translation entry timeouts because each entry contains more context about the traffic that is using it. Non-DNS UDP translations time out after 5 minutes, and DNS times out in 1 minute. TCP translations time out in 24 hours, unless an RST or FIN flag is seen on the stream, in which case they will time out in 1 minute.

Examples

The following example causes UDP port translation entries to time out after 10 minutes:

```
ip nat translation udp-timeout 600
```

Related Commands

| Command | Description |
|-----------------------------------|--|
| clear ipv6 nat translation | Clears dynamic NAT-PT translations from the translation table. |
| show ipv6 nat translations | Displays active NAT-PT translations. |

ipv6 nat v4v6 pool

To define a pool of IPv6 addresses for Network Address Translation - Protocol Translation (NAT-PT), use the **ipv6 nat v4v6 pool** command in global configuration mode. To remove one or more addresses from the pool, use the **no** form of this command.

ipv6 nat v4v6 pool *name start-ipv6 end-ipv6 prefix-length prefix-length*

no ipv6 nat v4v6 pool *name start-ipv6 end-ipv6 prefix-length prefix-length*

Syntax Description

| | |
|----------------------|---|
| <i>name</i> | Name of the pool. |
| <i>start-ipv6</i> | Starting IPv6 address that defines the range of IPv6 addresses in the address pool. |
| <i>end-ipv6</i> | Ending IPv6 address that defines the range of IPv6 addresses in the address pool. |
| prefix-length | Number that indicates how many bits of the address indicate the network. |
| <i>prefix-length</i> | Specify the subnet of the network to which the pool addresses belong. |

Defaults

No pool of addresses is defined.

Command Modes

Global configuration

Command History

| Release | Modification |
|-----------|------------------------------|
| 12.2(13)T | This command was introduced. |

Usage Guidelines

This command defines a pool of IPv6 addresses using start address, end address, and prefix length. The pool is used when NAT-PT needs a dynamic mapping of an IPv6 address to translate an IPv4 address.

Examples

The following example configures a dynamic NAT-PT mapping to translate IPv4 addresses to IPv6 addresses using a pool of IPv6 addresses named v6pool. The packets to be translated by NAT-PT are filtered using an access list named pt-list2. One static NAT-PT mapping is configured to access a Domain Naming System (DNS) server. Ethernet interface 3/1 is an IPv6-only host and Ethernet interface 3/3 is an IPv4-only host.

```
interface Ethernet3/1
  ipv6 address 2001:0DB8:AABB:1::9/64
  ipv6 enable
  ipv6 nat
!
interface Ethernet3/3
  ip address 192.168.30.9 255.255.255.0
  ipv6 nat
!
ipv6 nat v4v6 source list pt-list2 pool v6pool
ipv6 nat v4v6 pool v6pool 2001:0DB8:EEFF::1 2001:0DB8:EEFF::2 prefix-length 128
ipv6 nat v6v4 source 2001:0DB8:AABB:1::1 10.21.8.0
```

```
ipv6 nat prefix 2001:0DB8:EEFF::/96
!  
access-list pt-list2 permit 192.168.30.0 0.0.0.255
```

Related Commands

| Command | Description |
|------------------------------------|--|
| clear ipv6 nat translations | Clears dynamic NAT-PT translations from the translation table. |
| show ipv6 nat translations | Displays active NAT-PT translations. |

ipv6 nat v4v6 source

To configure IPv4 to IPv6 address translation using Network Address Translation - Protocol Translation (NAT-PT), use the **ipv6 nat v4v6 source** command in global configuration mode. To remove the static translation or remove the dynamic association to a pool, use the **no** form of this command.

```

ipv6 nat v4v6 source {list {access-list-number | name} pool name | ipv4-address ipv6-address}
no ipv6 nat v4v6 source {list {access-list-number | name} pool name | ipv4-address ipv6-address}
  
```

| | | |
|---------------------------|---------------------------------------|---|
| Syntax Description | list <i>access-list-number</i> | Standard IP access list number. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool. |
| | list <i>name</i> | Name of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool. |
| | pool <i>name</i> | Name of the pool from which global IP addresses are allocated dynamically. |
| | <i>ipv4-address</i> | Sets up a single static translation. This argument establishes the local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or obsolete. |
| | <i>ipv6-address</i> | Sets up a single static translation. This argument establishes the globally unique IP address of an inside host as it appears to the outside world. |

Defaults No NAT-PT translation of IPv4 to IPv6 addresses occurs.

Command Modes Global configuration

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 12.2(13)T | This command was introduced. |

Usage Guidelines This command has two forms: dynamic and static address translation. The form with an IPv6 access list establishes dynamic translation. Packets from IPv4 addresses that match the standard access list are translated using IPv6 addresses allocated from the pool named with the **ipv6 nat v4v6 pool** command. The access list is used to specify which traffic is to be translated.

Alternatively, the syntax form using the *ipv4-address* and *ipv6-address* arguments establishes a single static translation.

Examples The following example configures a dynamic NAT-PT mapping to translate IPv4 addresses to IPv6 addresses using a pool of IPv6 addresses named v6pool. The packets to be translated by NAT-PT are filtered using an access list named pt-list2. Ethernet interface 3/1 is an IPv6-only host and Ethernet interface 3/3 is an IPv4-only host.

```

interface Ethernet3/1
  ipv6 address 2001:0DB8:AABB:1::9/64
  ipv6 enable
  ipv6 nat
!
interface Ethernet3/3
  ip address 192.168.30.9 255.255.255.0
  ipv6 nat
!
ipv6 nat v4v6 source list pt-list2 pool v6pool
ipv6 nat v4v6 pool v6pool 2001:0DB8:EEFF::1 2001:0DB8:EEFF::2 prefix-length 128
ipv6 nat prefix 3ffe:c00:yyyy::/96
!
access-list pt-list2 permit 192.168.30.0 0.0.0.255

```

The following example shows a static translation where the IPv4 address 192.168.30.1 is translated into the IPv6 address 2001:0DB8:EEFF::2:

```

ipv6 nat v4v6 source 192.168.30.1 2001:0DB8:EEFF::2

```

Related Commands

| Command | Description |
|-----------------------------------|--|
| clear ipv6 nat translation | Clears dynamic NAT-PT translations from the translation state table. |
| ipv6 nat v4v6 pool | Defines a pool of IPv6 addresses for NAT-PT. |
| ipv6 nat v6v4 source | Enables NAT-PT for an IPv6 source address. |
| show ipv6 nat translations | Displays active NAT-PT translations. |

ipv6 nat v6v4 pool

To define a pool of IPv4 addresses for Network Address Translation - Protocol Translation (NAT-PT), use the **ipv6 nat v6v4 pool** global configuration command. To remove one or more addresses from the pool, use the **no** form of this command.

ipv6 nat v6v4 pool *name start-ipv4 end-ipv4 prefix-length prefix-length*

no ipv6 nat v6v4 pool *name start-ipv4 end-ipv4 prefix-length prefix-length*

Syntax Description

| | |
|----------------------|---|
| <i>name</i> | Name of the pool. |
| <i>start-ipv4</i> | Starting IPv4 address that defines the range of IPv4 addresses in the address pool. |
| <i>end-ipv4</i> | Ending IPv4 address that defines the range of IPv4 addresses in the address pool. |
| prefix-length | Number that indicates how many bits of the address indicate the network. |
| <i>prefix-length</i> | Specify the subnet of the network to which the pool addresses belong. |

Defaults

No pool of addresses is defined.

Command Modes

Global configuration

Command History

| Release | Modification |
|-----------|------------------------------|
| 12.2(13)T | This command was introduced. |

Usage Guidelines

This command defines a pool of IPv4 addresses using start address, end address, and prefix length. The pool is used when NAT-PT needs a dynamic mapping of IPv4 addresses to translate IPv6 addresses.

Examples

The following example configures a dynamic NAT-PT mapping to translate IPv6 addresses to IPv4 addresses using a pool of IPv4 addresses named v4pool. The packets to be translated by NAT-PT are filtered using an IPv6 access list named pt-list1. One static NAT-PT mapping is configured to access a Domain Naming System (DNS) server. Ethernet interface 3/1 is an IPv6-only host and Ethernet interface 3/3 is an IPv4-only host.

```
interface Ethernet3/1
  ipv6 address 2001:0DB8:AABB:1::9/64
  ipv6 enable
  ipv6 nat
!
interface Ethernet3/3
  ip address 192.168.30.9 255.255.255.0
  ipv6 nat
!
ipv6 nat v4v6 source 192.168.30.1 2001:0DB8:EEFF::2
ipv6 nat v6v4 source list pt-list1 pool v4pool
ipv6 nat v6v4 pool v4pool 10.21.8.1 10.21.8.10 prefix-length 24
```

```
ipv6 nat prefix 2001:0DB8:EEFF::/96
!
ipv6 access-list pt-list1
 permit ipv6 2001:0DB8:AABB:1::/64 any
```

Related Commands

| Command | Description |
|------------------------------------|--|
| clear ipv6 nat translations | Clears dynamic NAT-PT translations from the translation table. |
| show ipv6 nat translations | Displays active NAT-PT translations. |

ipv6 nat v6v4 source

To configure IPv6 to IPv4 address translation using Network Address Translation - Protocol Translation (NAT-PT), use the **ipv6 nat v6v4 source** command in global configuration mode. To remove the static translation or remove the dynamic association to a pool, use the **no** form of this command.

```

ipv6 nat v6v4 source {list access-list-name pool name | route-map map-name pool name |
  ipv6-address ipv4-address} [overload]
  
```

```

no ipv6 nat v6v4 source {list access-list-name pool name | route-map map-name pool name |
  ipv6-address ipv4-address} [overload]
  
```

Syntax Description

| | |
|-------------------------------------|--|
| list <i>access-list-name</i> | IPv6 access list name. Packets with source addresses that pass the access list are translated using global addresses from the named pool. |
| route-map <i>map-name</i> | Sets up a single static translation. This keyword and argument combination establishes the globally unique IP address assigned to a host on the outside network by its owner. It was allocated from globally routable network space. |
| pool <i>name</i> | Name of the pool from which global IP addresses are allocated dynamically. |
| <i>ipv6-address</i> | Sets up a single static translation. This argument establishes the globally unique IP address of an inside host as it appears to the outside world. |
| <i>ipv4-address</i> | Sets up a single static translation. This argument establishes the local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or obsolete. |
| overload | Enables multiplexing of IPv6 addresses to a single IPv4 address for TCP, UDP, and ICMP. |

Defaults

No NAT-PT translation of IPv6 to IPv4 addresses occurs.

Command Modes

Global configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(13)T | This command was introduced. |
| 12.3(2)T | The overload keyword was added to support Port Address Translation (PAT), or Overload, multiplexing multiple IPv6 addresses to a single IPv4 address or to an IPv4 address pool. |

Usage Guidelines

Dynamic and Static Address Translation

This command has two forms: dynamic and static address translation. The form with an IPv6 access list establishes dynamic translation. Packets from IPv6 addresses that match the IPv6 access list are translated using IPv4 addresses allocated from the pool named with the **ipv6 nat v6v4 pool** command. The access list is used to specify which traffic is to be translated.

Alternatively, the syntax form using the *ipv6-address* and *ipv4-address* arguments establishes a single static translation.

Port Address Translation

When used for PAT, the command can be used for a single IPv4 interface or for a pool of IPv4 interfaces.

Examples

Dynamic Mapping to a Pool of IPv4 Addresses Example

The following example configures a dynamic NAT-PT mapping to translate IPv6 addresses to IPv4 addresses using a pool of IPv4 addresses named v4pool. The packets to be translated by NAT-PT are filtered using an IPv6 access list named pt-list1. Ethernet interface 3/1 is an IPv6-only host and Ethernet interface 3/3 is an IPv4-only host.

```
interface Ethernet3/1
  ipv6 address3 ffe:aaaa:bbbb:1::9/64
  ipv6 enable
  ipv6 nat
!
interface Ethernet3/3
  ip address 192.168.30.9 255.255.255.0
  ipv6 nat
!
ipv6 nat v6v4 source list pt-list1 pool v4pool
ipv6 nat v6v4 pool v4pool 10.21.8.1 10.21.8.10 prefix-length 24
ipv6 nat prefix 3ffe:c00:::/96
!
ipv6 access-list pt-list1
  permit ipv6 3ffe:aaaa:bbbb:1::/64 any
```

Static Translation for a Single Address Example

The following example shows a static translation where the IPv6 address 3ffe:aaaa:bbbb:1::1 is translated into the IPv4 address 10.21.8.10:

```
ipv6 nat v6v4 source 3ffe:aaaa:bbbb:1::1 10.21.8.10
```

Port Address Translation to a Single Address Example

```
ipv6 nat v6v4 pool v6pool 128.1.1.1 128.1.1.10 subnetmask 255.255.255.0
ipv6 nat v6v4 source list v6list interface e1 overload
ipv6 accesslist v6list
  permit 3000::/64 any
```

Related Commands

| Command | Description |
|-----------------------------------|--|
| clear ipv6 nat translation | Clears dynamic NAT-PT translations from the translation state table. |
| debug ipv6 nat | Diaplays debugging messages for NAT-PT. |
| ipv6 nat v6v4 pool | Defines a pool of IPv4 addresses for NAT-PT. |
| ipv6 nat v4v6 source | Enables NAT-PT for an IPv4 source address. |
| show ipv6 nat translations | Displays active NAT-PT translations. |

ipv6 nd dad attempts

To configure the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on the unicast IPv6 addresses of the interface, use the **ipv6 nd dad attempts** command in interface configuration mode. To return the number of messages to the default value, use the **no** form of this command.

ipv6 nd dad attempts *value*

no ipv6 nd dad attempts *value*

Syntax Description

| | |
|--------------|--|
| <i>value</i> | The number of neighbor solicitation messages. The acceptable range is from 0 to 600. Configuring a value of 0 disables duplicate address detection processing on the specified interface; a value of 1 configures a single transmission without follow-up transmissions. Default is one message. |
|--------------|--|

Defaults

Duplicate address detection on unicast IPv6 addresses with the sending of one neighbor solicitation message is enabled.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(4)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

Duplicate address detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses.

The DupAddrDetectTransmits node configuration variable (as specified in RFC 2462, *IPv6 Stateless Address Autoconfiguration*) is used to automatically determine the number of consecutive neighbor solicitation messages that are sent on an interface while duplicate address detection is performed on a tentative unicast IPv6 address.

The interval between duplicate address detection, neighbor solicitation messages (the duplicate address detection timeout interval) is specified by the neighbor discovery-related variable RetransTimer (as specified in RFC 2461, *Neighbor Discovery for IP Version 6 [IPv6]*), which is used to determine the time between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. This is the same management variable used to specify the interval for neighbor solicitation messages during address resolution and neighbor unreachability detection. Use the **ipv6 nd ns-interval** command to configure the interval between neighbor solicitation messages that are sent during duplicate address detection.

Duplicate address detection is suspended on interfaces that are administratively “down.” While an interface is administratively “down,” the unicast IPv6 addresses assigned to the interface are set to a pending state. Duplicate address detection is automatically restarted on an interface when the interface returns to being administratively “up.”


Note

An interface returning to administratively “up” restarts duplicate address detection for all of the unicast IPv6 addresses on the interface. While duplicate address detection is performed on the link-local address of an interface, the state for the other IPv6 addresses is still set to TENTATIVE. When duplicate address detection is completed on the link-local address, duplicate address detection is performed on the remaining IPv6 addresses.

When duplicate address detection identifies a duplicate address, the state of the address is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message similar to the following is issued:

```
%IPV6-4-DUPLICATE: Duplicate address FE80::1 on Ethernet0
```

If the duplicate address is a global address of the interface, the address is not used and an error message similar to the following is issued:

```
%IPV6-4-DUPLICATE: Duplicate address 3000::4 on Ethernet0
```

All configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

Duplicate address detection is performed on all multicast-enabled IPv6 interfaces, including the following interface types:

- ATM permanent virtual circuit (PVC)
- Cisco High-Level Data Link Control (HDLC)
- Ethernet, Fast Ethernet, and Gigabit Ethernet
- FDDI
- Frame Relay PVC
- Point-to-point links
- PPP

Examples

The following example configures five consecutive neighbor solicitation messages to be sent on Ethernet interface 0 while duplicate address detection is being performed on the tentative unicast IPv6 address of the interface. The example also disables duplicate address detection processing on Ethernet interface 1.

```
Router(config)# interface ethernet 0
Router(config-if)# ipv6 nd dad attempts 5
```

```
Router(config)# interface ethernet 1
Router(config-if)# ipv6 nd dad attempts 0
```



Note

Configuring a value of 0 with the **ipv6 nd dad attempts** interface configuration command disables duplicate address detection processing on the specified interface; a value of 1 configures a single transmission without follow-up transmissions. The default is one message.

To display the state (OK, TENTATIVE, or DUPLICATE) of the unicast IPv6 address configured for an interface, to verify whether duplicate address detection is enabled on the interface, and to verify the number of consecutive duplicate address detection, neighbor solicitation messages that are being sent on the interface, enter the **show ipv6 interface EXEC** command:

```
Router# show ipv6 interface
```

```
Ethernet0 is up, line protocol is up
IPv6 is stalled, link-local address is FE80::1 [TENTATIVE]
Global unicast address(es):
  2000::1, subnet is 2000::/64 [TENTATIVE]
  3000::1, subnet is 3000::/64 [TENTATIVE]
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.

Ethernet1 is up, line protocol is up
IPv6 is stalled, link-local address is FE80::2
Global unicast address(es):
  2000::2, subnet is 2000::/64
  3000::3, subnet is 3000::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is disabled, number of DAD attempts: 0
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
```

Related Commands

| Command | Description |
|----------------------------|---|
| ipv6 nd ns-interval | Configures the interval between IPv6 neighbor solicitation transmissions on an interface. |
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 nd managed-config-flag

To set the “managed address configuration” flag in IPv6 router advertisements, use the **ipv6 nd managed-config-flag** command in interface configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Syntax Description

This command has no arguments or keywords.

Defaults

The “managed address configuration” flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

Setting the “managed address configuration” flag in IPv6 router advertisements indicates to attached hosts whether they should use stateful autoconfiguration to obtain addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain addresses. If the flag is not set, the attached hosts should not use stateful autoconfiguration to obtain addresses.

Hosts may use stateful and stateless address autoconfiguration simultaneously.

Examples

The following example configures the “managed address configuration” flag in IPv6 router advertisements on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd managed-config-flag
```

Related Commands

| Command | Description |
|-------------------------------------|---|
| ipv6 nd prefix-advertisement | Configures which IPv6 prefixes are included in IPv6 router advertisements |
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 nd ns-interval

To configure the interval between IPv6 neighbor solicitation retransmissions on an interface, use the **ipv6 nd ns-interval** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

Syntax Description

milliseconds The interval between IPv6 neighbor solicit transmissions. The acceptable range is from 1000 to 3600000 milliseconds.

Defaults

0 milliseconds (unspecified) is advertised in router advertisements and the value 1000 is used for the neighbor discovery activity of the router itself.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

This value will be included in all IPv6 router advertisements sent out this interface. Very short intervals are not recommended in normal IPv6 operation. When a nondefault value is configured, the configured time is both advertised and used by the router itself.

Examples

The following example configures an IPv6 neighbor solicit transmission interval of 9000 milliseconds for Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd ns-interval 9000
```

Related Commands

| Command | Description |
|----------------------------|--|
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 nd other-config-flag

To set the “other stateful configuration” flag in IPv6 router advertisements, use the **ipv6 nd other-config-flag** command in interface configuration mode. To clear the flag from IPv6 router advertisements, use the **no** form of this command.

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Syntax Description

This command has no arguments or keywords.

Defaults

The “other stateful configuration” flag is not set in IPv6 router advertisements.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The setting of the “other stateful configuration” flag in IPv6 router advertisements indicates to attached hosts how they can obtain autoconfiguration information other than addresses. If the flag is set, the attached hosts should use stateful autoconfiguration to obtain the other (nonaddress) information.



Note

If the “managed address configuration” flag is set using the **ipv6 nd managed-config-flag** command, then an attached host can use stateful autoconfiguration to obtain the other (nonaddress) information regardless of the setting of the “other stateful configuration” flag.

Examples

The following example configures the “other stateful configuration” flag in IPv6 router advertisements on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd other-config-flag
```

Related Commands

| Command | Description |
|------------------------------------|--|
| ipv6 nd managed-config-flag | Sets the “managed address configuration” flag in IPv6 router advertisements. |
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 nd prefix

To configure which IPv6 prefixes are included in IPv6 router advertisements, use the **ipv6 nd prefix** command in interface configuration mode. To remove the prefixes, use the **no** form of this command.

ipv6 nd prefix *ipv6-prefix/prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]]

no ipv6 nd prefix *ipv6-prefix/prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]]

| Syntax Description | | |
|--|--|--|
| <i>ipv6-prefix</i> | | The IPv6 network number to include in router advertisements. 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> | | The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |
| default | | Default values are used. |
| <i>valid-lifetime</i> | | The amount of time (in seconds) that the specified IPv6 prefix is advertised as being valid. |
| <i>preferred-lifetime</i> | | The amount of time (in seconds) that the specified IPv6 prefix is advertised as being preferred. |
| at <i>valid-date preferred-date</i> | | The date and time at which the lifetime and preference expire. The prefix is valid until this specified date and time are reached. Dates are expressed in the form <i>date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire</i> |
| infinite | | (Optional) The valid lifetime does not expire. |
| no-advertise | | (Optional) The prefix is not advertised. |
| off-link | | (Optional) Indicates that the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link. This prefix should not be used for <i>onlink</i> determination. |
| no-autoconfig | | (Optional) Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration. |

Defaults

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2592000 seconds (30 days) and a preferred lifetime of 604800 seconds (7 days), and with both the “onlink” and “autoconfig” flags set.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(13)T | This command was introduced. This command replaces the ipv6 nd prefix-advertisement command. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

This command allows control over the individual parameters per prefix, including whether or not the prefix should be advertised.

By default, prefixes configured as addresses on an interface using the **ipv6 address** command are advertised in router advertisements. If you configure prefixes for advertisement using the **ipv6 nd prefix** command, then only these prefixes are advertised.

Default Parameters

The default keyword can be used to set default parameters for all prefixes.

Prefix Lifetime and Expiration

A date can be set to specify the expiration of a prefix. The valid and preferred lifetimes are counted down in real time. When the expiration date is reached, the prefix will no longer be advertised.

Onlink

When onlink is “on” (by default), the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link.

Auto Configuration

When autoconfig is “on” (by default), it indicates to hosts on the local link that the specified prefix can be used for IPv6 autoconfiguration.

Examples

The following example includes the IPv6 prefix 2001:0DB8::/35 in router advertisements sent out Ethernet interface 0/0 with a valid lifetime of 1000 seconds, a preferred lifetime of 900 seconds, and both the “onlink” and “autoconfig” flags set:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd prefix 2001:0DB8::/35 1000 900 onlink autoconfig
```

Related Commands

| Command | Description |
|------------------------------------|--|
| ipv6 address link-local | Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface. |
| ipv6 address eui-64 | Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address. |
| ipv6 nd managed-config-flag | Sets the “managed address configuration” flag in IPv6 router advertisements. |
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 nd prefix-advertisement



Note

Effective with Cisco IOS Release 12.2(13)T, the `ipv6 nd prefix-advertisement` command is replaced by the `ipv6 nd prefix` command. See the `ipv6 nd prefix` command for more information.

To configure which IPv6 prefixes are included in IPv6 router advertisements, use the `ipv6 nd prefix-advertisement` command in interface configuration mode. To remove the prefixes, use the `no` form of this command.

ipv6 nd prefix-advertisement *ipv6-prefix/prefix-length valid-lifetime preferred-lifetime* [**onlink**] [**autoconfig**]

no ipv6 nd prefix-advertisement *ipv6-prefix/prefix-length*

Syntax Description

| | |
|---------------------------|--|
| <i>ipv6-prefix</i> | The IPv6 network number to include in router advertisements. 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> | The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |
| <i>valid-lifetime</i> | The amount of time (in seconds) that the specified IPv6 prefix is advertised as being valid. |
| <i>preferred-lifetime</i> | The amount of time (in seconds) that the specified IPv6 prefix is advertised as being preferred. |
| onlink | (Optional) Indicates that the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link. |
| autoconfig | (Optional) Indicates to hosts on the local link that the specified prefix can be used for IPv6 autoconfiguration. |

Defaults

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2592000 seconds (30 days) and a preferred lifetime of 604800 seconds (7 days), and with both the “onlink” and “autoconfig” flags set.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|---|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(13)T | This command was replaced by the <code>ipv6 nd prefix</code> command. |

Usage Guidelines

By default, prefixes configured on an interface using the **ipv6 address** command are advertised with “onlink” and “autoconfiguration” flags set. If you configure prefixes for advertisement using the **ipv6 nd prefix-advertisement** command, then only these prefixes are advertised.

Examples

The following example includes the IPv6 prefix 2001:0DB8::/35 in router advertisements sent out Ethernet interface 0/0 with a valid lifetime of 1000 seconds, a preferred lifetime of 900 seconds, and both the “onlink” and “autoconfig” flags set:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd prefix-advertisement 2001:0DB8::/35 1000 900 onlink autoconfig
```

Related Commands

| Command | Description |
|------------------------------------|--|
| ipv6 address link-local | Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface. |
| ipv6 address eui-64 | Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address. |
| ipv6 nd managed-config-flag | Sets the “managed address configuration” flag in IPv6 router advertisements. |
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 nd ra-interval

To configure the interval between IPv6 router advertisement transmissions on an interface, use the **ipv6 nd ra-interval** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ra-interval *seconds*

no ipv6 nd ra-interval

| | | |
|---------------------------|----------------|--|
| Syntax Description | <i>seconds</i> | The interval between IPv6 router advertisement transmissions (in seconds). |
|---------------------------|----------------|--|

| | |
|-----------------|-------------|
| Defaults | 200 seconds |
|-----------------|-------------|

| | |
|----------------------|-------------------------|
| Command Modes | Interface configuration |
|----------------------|-------------------------|

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

| | |
|-------------------------|---|
| Usage Guidelines | The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the router is configured as a default router by using the ipv6 nd ra-lifetime command. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the specified value. |
|-------------------------|---|

| | |
|-----------------|---|
| Examples | The following example configures an IPv6 router advertisement interval of 201 seconds for Ethernet interface 0/0: |
|-----------------|---|

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd ra-interval 201
```

| Related Commands | Command | Description |
|------------------|----------------------------|--|
| | ipv6 nd ra-lifetime | Configures the lifetime of an IPv6 router advertisement. |
| | show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 nd ra-lifetime

To configure the “router lifetime” value in IPv6 router advertisements on an interface, use the **ipv6 nd ra-lifetime** command in interface configuration mode. To restore the default lifetime, use the **no** form of this command.

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime

| | | |
|---------------------------|---------|---|
| Syntax Description | seconds | The validity of this router as a default router on this interface (in seconds). |
|---------------------------|---------|---|

| | |
|-----------------|--------------|
| Defaults | 1800 seconds |
|-----------------|--------------|

| | |
|----------------------|-------------------------|
| Command Modes | Interface configuration |
|----------------------|-------------------------|

| | | |
|------------------------|----------------|--|
| Command History | Release | Modification |
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

| | |
|-------------------------|---|
| Usage Guidelines | The “router lifetime” value is included in all IPv6 router advertisements sent out the interface. The value indicates the usefulness of the router as a default router on this interface. Setting the value to 0 indicates that the router should not be considered a default router on this interface. The “router lifetime” value can be set to a non zero value to indicate that it should be considered a default router on this interface. The non zero value for the “router lifetime” value should not be less than the router advertisement interval. |
|-------------------------|---|

| | |
|-----------------|--|
| Examples | The following example configures an IPv6 router advertisement lifetime of 1801 seconds for Ethernet interface 0/0: |
|-----------------|--|

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd ra-lifetime 1801
```

| | | |
|-------------------------|----------------------------|--|
| Related Commands | Command | Description |
| | ipv6 nd ra-interval | Configures the interval between IPv6 router advertisement transmissions on an interface. |
| | show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 nd reachable-time

To configure the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred, use the **ipv6 nd reachable-time** command in interface configuration mode. To restore the default time, use the **no** form of this command.

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

| Syntax Description | <i>milliseconds</i> The amount of time that a remote IPv6 node is considered reachable (in milliseconds). | | | | | | | | | | | |
|---------------------|--|--|---------|--------------|---------------------|--|------------|--|-----------|---|-----------|---|
| Defaults | 0 milliseconds (unspecified) is advertised in router advertisements and the value 30000 (30 seconds) is used for the neighbor discovery activity of the router itself. | | | | | | | | | | | |
| Command Modes | Interface configuration | | | | | | | | | | | |
| Command History | <table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.2(2)T</td><td>This command was introduced.</td></tr><tr><td>12.0(21)ST</td><td>This command was integrated into Cisco IOS Release 12.0(21)ST.</td></tr><tr><td>12.0(22)S</td><td>This command was integrated into Cisco IOS Release 12.0(22)S.</td></tr><tr><td>12.2(14)S</td><td>This command was integrated into Cisco IOS Release 12.2(14)S.</td></tr></table> | | Release | Modification | 12.2(2)T | This command was introduced. | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| Release | Modification | | | | | | | | | | | |
| 12.2(2)T | This command was introduced. | | | | | | | | | | | |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. | | | | | | | | | | | |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. | | | | | | | | | | | |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. | | | | | | | | | | | |
| Usage Guidelines | <p>The configured time enables the router to detect unavailable neighbors. Shorter configured times enable the router to detect unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.</p> <p>The configured time is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value. A value of 0 means indicates that the configured time is unspecified by this router.</p> | | | | | | | | | | | |
| Examples | <p>The following example configures an IPv6 reachable time of 1,700,000 milliseconds for Ethernet interface 0/0:</p> <pre>Router(config)# interface ethernet 0/0 Router(config-if)# ipv6 nd reachable-time 1700000</pre> | | | | | | | | | | | |
| Related Commands | <table><tr><th>Command</th><th>Description</th></tr><tr><td>show ipv6 interface</td><td>Displays the usability status of interfaces configured for IPv6.</td></tr></table> | | Command | Description | show ipv6 interface | Displays the usability status of interfaces configured for IPv6. | | | | | | |
| Command | Description | | | | | | | | | | | |
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. | | | | | | | | | | | |

ipv6 nd suppress-ra

To suppress IPv6 router advertisement transmissions on a LAN interface, use the **ipv6 nd suppress-ra** command in interface configuration mode. To reenable the sending of IPv6 router advertisement transmissions on a LAN interface, use the **no** form of this command.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Syntax Description

This command has no arguments or keywords.

Defaults

IPv6 router advertisements are automatically sent on Ethernet and FDDI interfaces if IPv6 unicast routing is enabled on the interfaces. IPv6 router advertisements are not sent on other types of interfaces.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

Use the **no ipv6 nd suppress-ra** command to enable the sending of IPv6 router advertisement transmissions on non-LAN interface types (for example, serial or tunnel interfaces).

Examples

The following example suppresses IPv6 router advertisements on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd suppress-ra
```

The following example enables the sending of IPv6 router advertisements on serial interface 0/1:

```
Router(config)# interface serial 0/1
Router(config-if)# no ipv6 nd suppress-ra
```

Related Commands

| Command | Description |
|----------------------------|--|
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 neighbor

To configure a static entry in the IPv6 neighbor discovery cache, use the **ipv6 neighbor** command in global configuration mode. To remove a static IPv6 entry from the IPv6 neighbor discovery cache, use the **no** form of this command.

ipv6 neighbor *ipv6-address interface-type interface-number hardware-address*

no ipv6 neighbor *ipv6-address interface-type interface-number*

Syntax Description

| | |
|-------------------------|---|
| <i>ipv6-address</i> | The IPv6 address that corresponds to the local data-link address. 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>interface-type</i> | The specified interface type. For supported interface types, use the question mark (?) online help function. |
| <i>interface-number</i> | The specified interface number. |
| <i>hardware-address</i> | The local data-link address (a 48-bit address). |

Defaults

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(8)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **ipv6 neighbor** command is similar to the **arp** (global) command.

If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry.

Use the **show ipv6 neighbors** command to view static entries in the IPv6 neighbor discovery cache. A static entry in the IPv6 neighbor discovery cache can have one of the following states:

- INCMP (Incomplete)—The interface for this entry is down.
- REACH (Reachable)—The interface for this entry is up.



Note Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP (Incomplete) and REACH (Reachable) states are different for dynamic and static cache entries. See the **show ipv6 neighbors** command for descriptions of the INCMP (Incomplete) and REACH (Reachable) states for dynamic cache entries.

The **clear ipv6 neighbors** command deletes all entries in the IPv6 neighbor discovery cache, except static entries. The **no ipv6 neighbor** command deletes a specified static entry from the neighbor discovery cache; the command does not remove dynamic entries—learned from the IPv6 neighbor discovery process—from the cache. Disabling IPv6 on an interface by using the **no ipv6 enable** command or the **no ipv6 unnumbered** command deletes all IPv6 neighbor discovery cache entries configured for that interface, except static entries (the state of the entry changes to INCMP [Incomplete]).

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.



Note Static entries for IPv6 neighbors can be configured only on IPv6-enabled LAN and ATM LAN Emulation interfaces.

Examples

The following example configures a static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8::45A and link-layer address 0002.7D1A.9472 on Ethernet interface 1:

```
Router(config)# ipv6 neighbor 2001:0DB8::45A ethernet1 0002.7D1A.9472
```

Related Commands

| Command | Description |
|-----------------------------|--|
| clear ipv6 neighbors | Deletes all entries in the IPv6 neighbor discovery cache, except static entries. |
| show ipv6 neighbors | Displays IPv6 neighbor discovery cache information. |

ipv6 ospf area

To enable OSPF for IPv6 on an interface, use the **ipv6 ospf area** command in interface configuration mode. To disable OSPF routing for interfaces defined, use the **no** form of this command.

ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

no ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

| | | |
|---------------------------|------------------------------------|---|
| Syntax Description | <i>process-id</i> | Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process. |
| | <i>area-id</i> | Area that is to be associated with the OSPF interface. |
| | instance <i>instance-id</i> | (Optional) Instance identifier. |

Defaults OSPF for IPv6 is disabled.

Command Modes Interface configuration

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines Before you enable OSPF for IPv6 on an interface using the **ipv6 ospf area** command, you must enable IPv6 on the interface, and you must enable IPv6 routing.

An OSPF instance (also known as an OSPF process) can be considered a logical router running OSPF in a physical router. Use the instance ID to control selection of other routers as your neighbors. You become neighbors only with routers that have the same instance ID.

In IPv6, users can configure many addresses on an interface. In OSPF for IPv6, all addresses on an interface are included by default. Users cannot select some addresses to be imported into OSPF for IPv6; either all addresses on an interface are imported, or no addresses on an interface are imported.

There is no limit to the number of **ipv6 ospf area** commands you can use on the router. You must have at least two interfaces configured for OSPF for IPv6 to run.

Examples The following example enables OSPF for IPv6 on an interface:

```

ipv6 unicast-routing
interface ethernet0/1
  ipv6 enable
  ipv6 ospf 1 area 0

```

```
ipv6 unicast-routing
interface ethernet0/2
  ipv6 enable
  ipv6 ospf 120 area 1.4.20.9 instance 2
```

Related Commands

| Command | Description |
|-------------------------|---|
| ipv6 router ospf | Enables OSPF router configuration mode. |

ipv6 ospf authentication

To specify the authentication type for an interface, use the **ipv6 ospf authentication** command in interface configuration mode. To remove the authentication type for an interface, use the **no** form of this command.

ipv6 ospf authentication ipsec spi md5 [*key-encryption-type*] *key* | **null**

no ipv6 ospf authentication ipsec spi spi

| Syntax Description | | |
|----------------------------|--|---|
| ipsec | | IP Security (IPSec). |
| spi <i>spi</i> | | Security policy index (SPI) value. The <i>spi</i> value must be a number from 256 to 4294967295, which is entered as a decimal. |
| md5 | | Enables Message Digest 5 (MD5) authentication. |
| <i>key-encryption-type</i> | | (Optional) One of two values can be entered: <ul style="list-style-type: none"> 0—The key is not encrypted. 7—The key is encrypted. |
| <i>key</i> | | Number used in the calculation of the message digest. The number is 32 hex digits (16 bytes) long. |
| null | | Used to override area authentication. |

Defaults No authentication.

Command Modes Interface configuration

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.3(4)T | This command was introduced. |

Usage Guidelines

The user needs to ensure that the same policy (the SPI and the key) is configured on all of the interfaces on the link. SPI values may automatically be used by other client applications, such as tunnels.

The policy database is common to all client applications on a box. This means that two IPSec clients, such as OSPF and a tunnel, cannot use the same SPI. Additionally, an SPI can only be used in one policy.

The null keyword is used to override existing area authentication. If area authentication is not configured, then it is not necessary to configure the interface with the **ipv6 ospf authentication null** command.

Examples The following example enables MD5 authentication and then overrides area authentication:

```
Router(config-if)# ipv6 ospf authentication ipsec spi 500 md5
1234567890abcdef1234567890abcdef
Router(config-if)# ipv6 ospf authentication null
```

ipv6 ospf cost

To explicitly specify the cost of sending a packet on an interface, use the **ipv6 ospf cost** command in interface configuration mode. To reset the interface cost to the default value, use the **no** form of this command.

```
ipv6 ospf cost interface-cost

no ipv6 ospf cost interface-cost
```

| | | |
|--------------------|----------------|--|
| Syntax Description | interface-cost | Unsigned integer value expressed as the link-state metric. It can be a value in the range from 1 to 65535. |
|--------------------|----------------|--|

| | |
|----------|--------------------------------------|
| Defaults | Default cost based on the bandwidth. |
|----------|--------------------------------------|

| | |
|---------------|-------------------------|
| Command Modes | Interface configuration |
|---------------|-------------------------|

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines

You can set the metric manually using this command, if you need to change the default. Using the **bandwidth** command changes the link cost as long as this command is not used.

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:

10⁸ / bandwidth

Using this formula, the default path costs were calculated as noted in the following list. If these values do not suit your network, you can use your own method of calculating path costs.

- 56-kbps serial link—Default cost is 1785.
- 64-kbps serial link—Default cost is 1562.
- T1 (1.544-Mbps serial link)—Default cost is 64.
- E1 (2.048-Mbps serial link)—Default cost is 48.
- 4-Mbps Token Ring—Default cost is 25.
- Ethernet—Default cost is 10.
- 16-Mbps Token Ring—Default cost is 6.
- FDDI—Default cost is 1.
- X25—Default cost is 5208.

- Asynchronous—Default cost is 10,000.
- ATM— Default cost is 1.

Examples

The following example sets the interface cost value to 65:

```
ipv6 ospf cost 65
```

ipv6 ospf database-filter all out

To filter outgoing link-state advertisements (LSAs) to an OSPF interface, use the **ipv6 ospf database-filter all out** command in interface configuration mode. To restore the forwarding of LSAs to the interface, use the **no** form of this command.

ipv6 ospf database-filter all out

no ipv6 ospf database-filter all out

Syntax Description

This command has no arguments or keywords.

Defaults

All outgoing LSAs are flooded to the interface.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-----------|---|
| 12.0(24)S | This command was introduced. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines

This command performs the same function that the **neighbor database-filter** command performs on a neighbor basis.

Examples

The following example prevents flooding of OSPF LSAs to broadcast, nonbroadcast, or point-to-point networks reachable through Ethernet interface 0:

```
interface ethernet 0
  ipv6 ospf database-filter all out
```

ipv6 ospf dead-interval

To set the time period for which hello packets must not be seen before neighbors declare the router down, use the **ipv6 ospf dead-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

ipv6 ospf dead-interval *seconds*

no ipv6 ospf dead-interval

| | | |
|---------------------------|----------------|---|
| Syntax Description | <i>seconds</i> | Specifies the interval (in seconds). The value must be the same for all nodes on the network. |
|---------------------------|----------------|---|

| | |
|-----------------|--|
| Defaults | Four times the interval set by the ipv6 ospf hello-interval command |
|-----------------|--|

| | |
|----------------------|-------------------------|
| Command Modes | Interface configuration |
|----------------------|-------------------------|

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

| | |
|-------------------------|---|
| Usage Guidelines | The interval is advertised in router hello packets. This value must be the same for all routers and access servers on a specific network. |
|-------------------------|---|

| | |
|-----------------|--|
| Examples | The following example sets the OSPF dead interval to 60 seconds: <pre>interface ethernet 1 ipv6 ospf dead-interval 60</pre> |
|-----------------|--|

| Related Commands | Command | Description |
|------------------|---------------------------------|--|
| | ipv6 ospf hello-interval | Specifies the interval between hello packets that the Cisco IOS software sends on the interface. |

ipv6 ospf demand-circuit

To configure OSPF to treat the interface as an OSPF demand circuit, use the **ipv6 ospf demand-circuit** command in interface configuration mode. To remove the demand circuit designation from the interface, use the **no** form of this command.

ipv6 ospf demand-circuit

no ipv6 ospf demand-circuit

Syntax Description

This command has no arguments or keywords.

Defaults

The circuit is not a demand circuit.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-----------|---|
| 12.0(24)S | This command was introduced. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines

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. 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.

Examples

The following example sets the configuration for an ISDN on-demand circuit:

```
interface BRI0
  ipv6 ospf 1 area 1
  ipv6 ospf demand-circuit
```

ipv6 ospf flood-reduction

To suppress the unnecessary flooding of link-state advertisements (LSAs) in stable topologies, use the **ipv6 ospf flood-reduction** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 ospf flood-reduction

no ipv6 ospf flood-reduction

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines All routers supporting the OSPF demand circuit are compatible and can interact with routers supporting flooding reduction.

Examples The following example suppresses the flooding of unnecessary LSAs on serial interface 0:

```
interface serial 0
  ipv6 ospf flood-reduction
```

| Related Commands | Command | Description |
|------------------|---------------------------------|--|
| | show ipv6 ospf interface | Displays OSPF-related interface information. |
| | show ipv6 ospf neighbor | Displays OSPF-neighbor information on a per-interface basis. |

ipv6 ospf hello-interval

To specify the interval between hello packets that the Cisco IOS software sends on the interface, use the **ipv6 ospf hello-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

ipv6 ospf hello-interval *seconds*

no ipv6 ospf hello-interval

| | | |
|--------------------|----------------|--|
| Syntax Description | <i>seconds</i> | Specifies the interval (in seconds). The value must be the same for all nodes on a specific network. |
|--------------------|----------------|--|

| | |
|----------|--|
| Defaults | 10 seconds (Ethernet) 30 seconds (nonbroadcast) |
|----------|--|

| | |
|---------------|-------------------------|
| Command Modes | Interface configuration |
|---------------|-------------------------|

| | | |
|-----------------|-----------|---|
| Command History | Release | Modification |
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

| | |
|------------------|---|
| Usage Guidelines | This value is advertised in the hello packets. The shorter the hello interval, the earlier topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network. |
|------------------|---|

| | |
|----------|---|
| Examples | The following example sets the interval between hello packets to 15 seconds: interface ethernet 1 ipv6 ospf hello-interval 15 |
|----------|---|

| | | |
|------------------|--------------------------------|--|
| Related Commands | Command | Description |
| | ipv6 ospf dead-interval | Sets the time period for which hello packets must not have been seen before neighbors declare the router down. |

ipv6 ospf mtu-ignore

To disable OSPF maximum transmission unit (MTU) mismatch detection on receiving database descriptor (DBD) packets, use the **ipv6 ospf mtu-ignore** command in interface configuration mode. To reset to default, use the **no** form of this command.

ipv6 ospf mtu-ignore

no ipv6 ospf mtu-ignore

Syntax Description

This command has no arguments or keywords.

Defaults

OSPF MTU mismatch detection is enabled.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-----------|---|
| 12.0(24)S | This command was introduced. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines

OSPF checks whether 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 IP MTU configured on the incoming interface, OSPF adjacency will not be established.

Examples

The following example disables MTU mismatch detection on receiving DBD packets:

```
interface serial 0/0
  ipv6 ospf mtu-ignore
```

ipv6 ospf name-lookup

To display OSPF router IDs as Domain Naming System (DNS) names, use the **ipv6 ospf name-lookup** command in global configuration mode. To stop displaying OSPF router IDs as DNS names, use the **no** form of this command.

ipv6 ospf name-lookup

no ipv6 ospf name-lookup

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled by default

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines This command makes it easier to identify a router because the router is displayed by name rather than by its router ID or neighbor ID.

Examples The following example configures OSPF to look up DNS names for use in all OSPF show EXEC command displays:

```
ipv6 ospf name-lookup
```

ipv6 ospf neighbor

To configure OSPF routers interconnecting to nonbroadcast networks, use the **ipv6 ospf neighbor** command in interface configuration mode. To remove a configuration, use the **no** form of this command.

ipv6 ospf neighbor *ipv6-address* [**priority number**] [**poll-interval seconds**] [**cost number**]
[**database-filter all out**]

no ipv6 ospf neighbor *ipv6-address* [**priority number**] [**poll-interval seconds**] [**cost number**]
[**database-filter all out**]

| | | |
|---------------------------|--------------------------------|---|
| Syntax Description | <i>ipv6-address</i> | Link-local IPv6 address of the neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| | priority number | (Optional) A number that indicates the router priority value of the nonbroadcast neighbor associated with the IPv6 prefix specified. The default is 0. |
| | poll-interval seconds | (Optional) A number value that represents the poll interval time (in seconds). RFC 2328 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes). This keyword does not apply to point-to-multipoint interfaces. |
| | cost number | (Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured will assume the cost of the interface, based on the ipv6 ospf cost command. |
| | database-filter all out | (Optional) Filters outgoing link-state advertisements (LSAs) to an OSPF neighbor. |

Defaults No configuration is specified.

Command Modes Interface configuration

| Command History | Release | Modification |
|------------------------|----------------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines X.25 and Frame Relay provide an optional broadcast capability that can be configured in the map to allow OSPF to run as a broadcast network. At the OSPF level you can configure the router as a broadcast network.

One neighbor entry must be included in the Cisco IOS software configuration for each known nonbroadcast network neighbor. The neighbor address must be a link-local address of the neighbor.

If a neighboring router has become inactive (hello packets have not been seen for the Router Dead Interval period), hello packets may need to be sent to the dead neighbor. These hello packets will be sent at a reduced rate called *Poll Interval*.

When the router first 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 will then start sending hello packets to all neighbors in order to form adjacencies.

The **priority** keyword does not apply to point-to-multipoint interfaces. For point-to-multipoint interfaces, the **cost** keyword and the *number* argument are the only options that are applicable. The **cost** keyword does not apply to nonbroadcast multiaccess (NBMA) networks.

Examples

The following example configures an OSPF neighboring router:

```
ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

ipv6 ospf network

To configure the OSPF network type to a type other than the default for a given medium, use the **ipv6 ospf network** command in interface configuration mode. To return to the default value, use the **no** form of this command.

```

ipv6 ospf network { broadcast | non-broadcast | { point-to-multipoint [non-broadcast] |
point-to-point } }

no ipv6 ospf network
  
```

| | | |
|---------------------------|---|--|
| Syntax Description | broadcast | Sets the network type to broadcast. |
| | non-broadcast | Sets the network type to nonbroadcast multiaccess (NBMA). |
| | point-to-multipoint [non-broadcast] | Sets the network type to point-to-multipoint. The optional non-broadcast keyword 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 Default depends on the network type.

Command Modes Interface configuration

| Command History | Release | Modification |
|------------------------|----------------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines Using this feature, you can configure broadcast networks as NBMA networks when, for example, routers in your network do not support multicast addressing. You can also configure NBMA networks (such as X.25, Frame Relay, and Switched Multimegabit Data Service [SMDS]) as broadcast networks. This feature saves you from needing to configure neighbors.

Configuring NBMA networks as either broadcast or nonbroadcast assumes that there are virtual circuits from every router to every router or fully meshed networks. However, the assumption is not true for other configurations, such as for 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 will go through the router that has virtual circuits to both routers. You need not configure neighbors when using this feature.

OSPF for IPv6 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.

Examples

The following example sets your OSPF network as a broadcast network:

```
interface serial 0
  ipv6 enable
  ipv6 ospf 1 area 0
  ipv6 ospf network broadcast
  encapsulation frame-relay
```

The following example illustrates a point-to-multipoint network with broadcast:

```
interface serial 0
  ipv6 enable
  ipv6 ospf 1 area 0
  encapsulation frame-relay
  ipv6 ospf cost 100
  ipv6 ospf network point-to-multipoint
  frame-relay map ipv6 FE80::A8BB:CCFF:FE00:C01 broadcast
  frame-relay map ipv6 FE80::A8BB:CCFF:FE00:C02 broadcast
  frame-relay local-dlci 200
  ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
  ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C02
```

Related Commands

| Command | Description |
|---------------------------|---|
| frame-relay map | Defines mapping between a destination protocol address and the DLCI used to connect to the destination address. |
| ipv6 ospf neighbor | Configures OSPF routers interconnecting to nonbroadcast networks. |
| x25 map | Sets up the LAN protocols-to-remote host mapping. |

ipv6 ospf priority

To set the router priority, which helps determine the designated router for this network, use the **ipv6 ospf priority** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf priority *number-value*

no ipv6 ospf priority *number-value*

| | | |
|---------------------------|---------------------|---|
| Syntax Description | <i>number-value</i> | A number value that specifies the priority of the router. The range is from 0 to 255. |
|---------------------------|---------------------|---|

| | |
|-----------------|---------------|
| Defaults | Priority of 1 |
|-----------------|---------------|

| | |
|----------------------|-------------------------|
| Command Modes | Interface configuration |
|----------------------|-------------------------|

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

| | |
|-------------------------|---|
| Usage Guidelines | 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 to point-to-point networks). |
|-------------------------|---|

This priority value is used when you configure OSPF for nonbroadcast networks using the **ipv6 ospf neighbor** command.

| | |
|-----------------|--|
| Examples | The following example sets the router priority value to 4: |
|-----------------|--|

```
interface ethernet 0
  ipv6 ospf priority 4
```

| | | |
|-------------------------|---------------------------|---|
| Related Commands | Command | Description |
| | ipv6 ospf network | Configures the OSPF network type to a type other than the default for a given medium. |
| | ipv6 ospf neighbor | Configures OSPF routers interconnecting to nonbroadcast networks. |

ipv6 ospf retransmit-interval

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface, use the **ipv6 ospf retransmit-interval** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf retransmit-interval *seconds*

no ipv6 ospf 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. The range is from 1 to 65535 seconds. The default is 5 seconds. |
|---------------------------|----------------|---|

| | |
|-----------------|-----------|
| Defaults | 5 seconds |
|-----------------|-----------|

| | |
|----------------------|-------------------------|
| Command Modes | Interface configuration |
|----------------------|-------------------------|

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

| | |
|-------------------------|---|
| Usage Guidelines | When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it will resend the LSA. |
| | The setting of this parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links. |

| | |
|-----------------|--|
| Examples | The following example sets the retransmit interval value to 8 seconds: |
|-----------------|--|

```
interface ethernet 2
  ipv6 ospf retransmit-interval 8
```


ipv6 ospf transmit-delay

To set the estimated time required to send a link-state update packet on the interface, use the **ip ospf transmit-delay** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf transmit-delay *seconds*

no ipv6 ospf transmit-delay

| | | |
|---------------------------|----------------|--|
| Syntax Description | <i>seconds</i> | Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second. |
|---------------------------|----------------|--|

| | |
|-----------------|----------|
| Defaults | 1 second |
|-----------------|----------|

| | |
|----------------------|-------------------------|
| Command Modes | Interface configuration |
|----------------------|-------------------------|

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines

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, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Examples

The following example sets the retransmit delay value to 3 seconds:

```
interface ethernet 0
  ipv6 ospf transmit-delay 3
```

ipv6 pim

To reenable IPv6 Protocol Independent Multicast (PIM) on a specified interface, use the **ipv6 pim** command in interface configuration mode. To disable PIM on a specified interface, use the **no** form of the command.

ipv6 pim

no ipv6 pim

Syntax Description

This command has no arguments or keywords.

Defaults

PIM is automatically enabled on every interface.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-----------|---|
| 12.3(2)T | This command was introduced. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

After a user has enabled the **ipv6 multicast-routing** command, PIM is enabled to run on every interface. Because PIM is enabled on every interface by default, use the **no** form of the **ipv6 pim** command to disable PIM on a specified interface. When PIM is disabled on an interface, it does not react to any host membership notifications from the Multicast Listener Discovery (MLD) protocol.

Examples

The following example turns off PIM on Fast Ethernet interface 1/0:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# no ipv6 pim
```

Related Commands

| Command | Description |
|-------------------------------|--|
| ipv6 multicast-routing | Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding. |

ipv6 pim accept-register

To accept or reject registers at the rendezvous point (RP), use the **ipv6 pim accept-register** command in global configuration mode. To return to the default value, use the **no** form of this command.

ipv6 pim accept-register {**list** *access-list* | **route-map** *map-name*}

no ipv6 pim accept-register {**list** *access-list* | **route-map** *map-name*}

Syntax Description

| | |
|----------------------------------|-------------------------------|
| list <i>access-list</i> | Defines the access list name. |
| route-map <i>map-name</i> | Defines the route map. |

Defaults

All sources are accepted at the RP.

Command Modes

Global configuration

Command History

| Release | Modification |
|-----------|--|
| 12.0(26)S | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines

Use the **ipv6 pim accept-register** command to configure a named access list or route-map with match attributes. When the permit conditions as defined by the *access-list* and *map-name* arguments are met, the register message is accepted. Otherwise, the register message is not accepted, and an immediate register-stop message is returned to the encapsulating designated router.

Examples

The following example shows how to filter on all sources that do not have a local multicast Border Gateway Protocol (MBGP) prefix:

```

ipv6 pim accept-register route-map reg-filter
route-map reg-filter permit 20
  match as-path 101
ip as-path access-list 101 permit
  
```

ipv6 pim dr-priority

To configure the designated router (DR) priority on a Protocol Independent Multicast (PIM) router, use the **ipv6 pim dr-priority** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 pim dr-priority *value*

no ipv6 pim dr-priority

| | | |
|--------------------|--------------|---|
| Syntax Description | <i>value</i> | An integer value to represent DR priority. Value range is from 0 to 4294967294. The default value is 1. |
|--------------------|--------------|---|

| | |
|----------|---------------------|
| Defaults | Default value is 1. |
|----------|---------------------|

| | |
|---------------|-------------------------|
| Command Modes | Interface configuration |
|---------------|-------------------------|

| | | |
|-----------------|-----------|---|
| Command History | Release | Modification |
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

| | |
|------------------|---|
| Usage Guidelines | <p>The ipv6 pim dr-priority command configures the neighbor priority used for PIM DR election. The router with the highest DR priority on an interface becomes the PIM DR. If several routers have the same priority, then the router with the highest IPv6 address on the interface becomes the DR.</p> <p>If a router does not include the DR priority option in its hello messages, then the router is considered to be the highest-priority router and becomes the DR. If several routers do not include the DR priority option in their hello messages, then the router with the highest IPv6 address becomes the DR.</p> |
|------------------|---|

| | |
|----------|--|
| Examples | <p>The following example configures the router to use DR priority 3:</p> <pre>Router(config)# interface FastEthernet 1/0 Router(config-if)# ipv6 pim dr-priority 3</pre> |
|----------|--|

| | | |
|------------------|--------------------------------|---|
| Related Commands | Command | Description |
| | ipv6 pim hello-interval | Configures the frequency of PIM hello messages on an interface. |

ipv6 pim hello-interval

To configure the frequency of Protocol Independent Multicast (PIM) hello messages on an interface, use the **ipv6 pim hello-interval** command in interface configuration mode. To return to the default interval, use the **no** form of this command.

ipv6 pim hello-interval *seconds*

no ipv6 pim hello-interval *seconds*

| | | |
|---------------------------|----------------|---|
| Syntax Description | <i>seconds</i> | Interval, in seconds, at which PIM hello messages are sent. |
|---------------------------|----------------|---|

| | |
|-----------------|--|
| Defaults | Hello messages are sent at 30-second intervals with small random jitter. |
|-----------------|--|

| | |
|----------------------|-------------------------|
| Command Modes | Interface configuration |
|----------------------|-------------------------|

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

| | |
|-------------------------|--|
| Usage Guidelines | Periodic hello messages are sent out at 30-second intervals with a small jitter. The ipv6 pim hello-interval command allows users to set a periodic interval. |
|-------------------------|--|

| | |
|-----------------|--|
| Examples | The following example sets the PIM hello message interval to 45 seconds: |
|-----------------|--|

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 pim hello-interval 45
```

| | | |
|-------------------------|--------------------------------|---|
| Related Commands | Command | Description |
| | ipv6 mld query-interval | Configures the frequency at which the Cisco IOS software sends MLD host-query messages. |
| | ipv6 pim dr-priority | Configures the DR priority on a PIM router. |
| | show ipv6 pim neighbor | Displays the PIM neighbors discovered by the Cisco IOS software. |

ipv6 pim join-prune-interval

To configure periodic join and prune announcement intervals for a specified interface, use the **ipv6 pim join-prune-interval** command in interface configuration mode. To return to the default value, use the **no** form of the command.

```
ipv6 pim join-prune-interval seconds

no ipv6 pim join-prune-interval seconds
```

| | | |
|--------------------|---------|---|
| Syntax Description | seconds | The join and prune announcement intervals, in number of seconds. The default value is 60 seconds. |
|--------------------|---------|---|

| | |
|----------|------------|
| Defaults | 60 seconds |
|----------|------------|

| | |
|---------------|-------------------------|
| Command Modes | Interface configuration |
|---------------|-------------------------|

| CommandHistory | Release | Modification |
|----------------|-----------|--|
| | 12.0(26)S | This command was introduced. |
| | 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

| | |
|------------------|---|
| Usage Guidelines | Periodic join and prune announcements are sent out at 60-second intervals. The ipv6 pim join-prune-interval command allows users to set a periodic interval. |
|------------------|---|

| | |
|----------|---|
| Examples | <p>The following example sets the join and prune announcement intervals to 75 seconds:</p> <pre>Router(config)# interface FastEthernet 1/0 Router(config-if)# ipv6 pim join-prune-interval 75</pre> |
|----------|---|

ipv6 pim rp embedded

To enable embedded rendezvous point (RP) support in IPv6 Protocol Independent Multicast (PIM), use the **ipv6 pim rp-embedded** command in global configuration mode. To disable embedded RP support, use the **no** form of this command.

ipv6 pim rp embedded

no ipv6 pim rp embedded

Syntax Description This command has no arguments or keywords.

Defaults Embedded RP support is enabled by default.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-----------|--|
| | 12.0(26)S | This command was introduced. |
| | 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines Because embedded RP support is enabled by default, users will generally use the **no** form of this command to turn off embedded RP support.

The **ipv6 pim rp embedded** command applies only to the embedded RP group ranges ff7X::/16 and fffX::/16. When enabled, the router parses groups in the embedded RP group ranges ff7X::/16 and fffX::/16, and extracts the RP to be used from the group address.

Examples The following example disables embedded RP support in IPv6 PIM:

```
no ipv6 pim rp embedded
```

ipv6 pim rp-address

To configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for a particular group range, use the **ipv6 pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

ipv6 pim rp-address *ipv6-address* [*group-access-list*]

no ipv6 pim rp-address *ipv6-address* [*group-access-list*]

| | | |
|---------------------------|--------------------------|---|
| Syntax Description | <i>ipv6-address</i> | The IPv6 address of a router to be a PIM RP. The <i>ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| | <i>group-access-list</i> | (Optional) Name of an access list that defines for which multicast groups the RP should be used. To support embedded RP, the router configured as the RP must use a configured access list that permits the embedded RP group ranges derived from the embedded RP address. Note that the embedded RP group ranges need not include all the scopes (for example, 3 through 7). |

| | |
|-----------------|--|
| Defaults | No PIM RPs are preconfigured. Embedded RP support is enabled by default when IPv6 PIM is enabled (where embedded RP support is provided). |
|-----------------|--|

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | Embedded RP support was added. |

| | |
|-------------------------|---|
| Usage Guidelines | When PIM is configured in sparse mode, you must choose one or more routers to operate as the RP. An RP is a single common root of a shared distribution tree and is statically configured on each router. |
| | Where embedded RP support is available, only the RP needs to be statically configured as the RP for the embedded RP ranges. No additional configuration is needed on other IPv6 PIM routers. The other routers will discover the RP address from the IPv6 group address. If these routers want to select a static RP instead of the embedded RP, the specific embedded RP group range must be configured in the access list of the static RP. |

The RP address is used by first-hop routers to send register packets on behalf of source multicast hosts. The RP address is also used by routers on behalf of multicast hosts that want to become members of a group. These routers send join and prune messages to the RP.

If the optional *group-access-list* argument is not specified, the RP is applied to the entire routable IPv6 multicast group range, excluding SSM, which ranges from FFX[3-f]::/8 to FF3X::/96. If the *group-access-list* argument is specified, the IPv6 address is the RP address for the group range specified in the *group-access-list* argument.

You can configure Cisco IOS software to use a single RP for more than one group. The conditions specified by the access list determine which groups the RP can be used for. If no access list is configured, the RP is used for all groups.

A PIM router can use multiple RPs, but only one per group.

Examples

The following example sets the PIM RP address to 2001::10:10 for all multicast groups:

```
Router(config)# ipv6 pim rp-address 2001::10:10
```

The following example sets the PIM RP address to 2001::10:10 for the multicast group FF04::/64 only:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 any ff04::/64
Router(config)# ipv6 pim rp-address 2001::10:10 acc-grp-1
```

The following example configures a group access list that permits the embedded RP ranges derived from the IPv6 RP address 2:2:2::2:

```
Router(config)# ipv6 pim rp-address 2:2:2::2 embd-ranges
Router(config)# ipv6 access-list embd-ranges
Router(config-ipv6-acl)# permit ipv6 any ff73:240:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff74:240:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff75:240:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff76:240:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff77:240:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff78:240:2:2::/96
```

ipv6 pim rp embedded

To enable embedded rendezvous point (RP) support in IPv6 Protocol Independent Multicast (PIM), use the **ipv6 pim rp-embedded** command in global configuration mode. To disable embedded RP support, use the **no** form of this command.

ipv6 pim rp embedded

no ipv6 pim rp embedded

Syntax Description

This command has no arguments or keywords.

Defaults

Embedded RP support is enabled by default.

Command Modes

Global configuration

Command History

| Release | Modification |
|-----------|------------------------------|
| 12.0(26)S | This command was introduced. |

Usage Guidelines

Because embedded RP support is enabled by default, users will generally use the **no** form of this command to turn off embedded RP support.

The **ipv6 pim rp embedded** command applies only to the embedded RP group ranges ff7X::/16 and fffX::/16. When enabled, the router parses groups in the embedded RP group ranges ff7X::/16 and fffX::/16, and extracts the RP to be used from the group address.

Examples

The following example disables embedded RP support in IPv6 PIM:

```
no ipv6 pim rp embedded
```

ipv6 pim spt-threshold infinity

To configure when a Protocol Independent Multicast (PIM) leaf router joins the shortest path tree (SPT) for the specified groups, use the **ipv6 pim spt-threshold infinity** command in global configuration mode. To restore the default value, use the **no** form of this command.

ipv6 pim spt-threshold infinity [**group-list** *access-list-name*]

no ipv6 pim spt-threshold infinity

Syntax Description

| | |
|--|---|
| group-list <i>access-list-name</i> | (Optional) Indicates to which groups the threshold applies. Must be a standard IPv6 access list name. If the value is omitted, the threshold applies to all groups. |
|--|---|

Defaults

When this command is not used, the PIM leaf router joins the SPT immediately after the first packet arrives from a new source. Once the router has joined the SPT, configuring the **ipv6 pim spt-threshold infinity** command will not cause it to switch to the shared tree.

Command Modes

Global configuration

Command History

| Release | Modification |
|-----------|---|
| 12.3(2)T | This command was introduced. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

Using the **ipv6 pim spt-threshold infinity** command enables all sources for the specified groups to use the shared tree. The **group-list** keyword indicates to which groups the SPT threshold applies.

The *access-list-name* argument refers to an IPv6 access list. When the *access-list-name* argument is specified with a value of 0, or the **group-list** keyword is not used, the SPT threshold applies to all groups. The default setting (that is, when this command is not enabled) is to join the SPT immediately after the first packet arrives from a new source.

Examples

The following example configures a PIM last-hop router to stay on the shared tree and not switch to the SPT for the group ff04::/64.:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 any FF04::/64
Router(config-ipv6-acl)# exit
Router(config)# ipv6 pim spt-threshold infinity group-list acc-grp-1
```

ipv6 prefix-list

To create an entry in an IPv6 prefix list, use the **ipv6 prefix-list** command in global configuration mode. To delete the entry, use the **no** form of this command.

```

ipv6 prefix-list list-name [seq seq-number] { deny ipv6-prefix/prefix-length | permit
ipv6-prefix/prefix-length | description text } [ge ge-value] [le le-value]

no ipv6 prefix-list list-name

```

Syntax Description

| | |
|--------------------------------|--|
| <i>list-name</i> | Name of the prefix list (cannot be the same as an existing access list). |
| seq <i>seq-number</i> | (Optional) Sequence number of the prefix list entry being configured. |
| deny | Denies networks that matches the condition. |
| permit | Permits networks that matches the condition. |
| <i>ipv6-prefix</i> | The IPv6 network assigned to the specified prefix list. 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> | The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |
| description <i>text</i> | A description of the prefix list that can be up to 80 characters in length. |
| ge <i>ge-value</i> | (Optional) Specifies a prefix length greater than or equal to the <i>ipv6-prefix/prefix-length</i> arguments. It is the lowest value of a range of the <i>length</i> (the “from” portion of the length range). |
| le <i>le-value</i> | (Optional) Specifies a prefix length less than or equal to the <i>ipv6-prefix/prefix-length</i> arguments. It is the highest value of a range of the <i>length</i> (the “to” portion of the length range). |

Defaults

No prefix list is created.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **ipv6 prefix-list** command is similar to the **ip prefix-list** command, except that it is IPv6-specific. To suppress networks from being advertised in updates, use the **distribute-list out** command.

The sequence number of a prefix list entry determines the order of the entries in the list. The router compares network addresses to the prefix list entries. The router begins the comparison at the top of the prefix list, with the entry having the lowest sequence number.

If multiple entries of a prefix list match a prefix, the entry with the lowest sequence number is considered the real match. Once a match or deny occurs, the router does not go through the rest of the prefix list. For efficiency, you may want to put the most common permits or denies near the top of the list, using the *seq-number* argument.

The **show ipv6 prefix-list** command displays the sequence numbers of entries.

IPv6 prefix lists are used to specify certain prefixes or a range of prefixes that must be matched before a permit or deny statement can be applied. Two operand keywords can be used to designate a range of prefix lengths to be matched. A prefix length of less than, or equal to, a value is configured with the **le** keyword. A prefix length greater than, or equal to, a value is specified using the **ge** keyword. The **ge** and **le** keywords can be used to specify the range of the prefix length to be matched in more detail than the usual *ipv6-prefix/prefix-length* argument. For a candidate prefix to match against a prefix list entry three conditions can exist:

- the candidate prefix must match the specified prefix list and prefix length entry
- the value of the optional **le** keyword specifies the range of allowed prefix lengths from the *prefix-length* argument up to, and including, the value of the **le** keyword
- the value of the optional **ge** keyword specifies the range of allowed prefix lengths from the value of the **ge** keyword up to, and including, 128.



Note

Note that the first condition must match before the other conditions take effect.

An exact match is assumed when the **ge** or **le** keywords are not specified. If only one keyword operand is specified then the condition for that keyword is applied, and the other condition is not applied. The *prefix-length* value must be less than the **ge** value. The **ge** value must be less than, or equal to, the **le** value. The **le** value must be less than or equal to 128.

Every IPv6 prefix list, including prefix lists that do not have any permit and deny condition statements, has an implicit deny any any statement as its last match condition.

Examples

The following example denies the default route `::/0`.

```
Router(config)# ipv6 prefix-list abc deny ::/0
```

The following example permits the prefix `2002::/16`:

```
Router(config)# ipv6 prefix-list abc permit 2002::/16
```

The following example shows how to specify a group of prefixes to accept any prefixes from prefix `5F00::/48` up to and including prefix `5F00::/64`.

```
Router(config)# ipv6 prefix-list abc permit 5F00::/48 le 64
```

The following example denies prefix lengths greater than 64 bits in routes that have the prefix `2001:0DB8::/64`.

```
Router(config)# ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
```

The following example permits mask lengths from 32 to 64 bits in all address space.

```
Router(config)# ipv6 prefix-list abc permit ::/0 ge 32 le 64
```

The following example denies mask lengths greater than 32 bits in all address space.

```
Router(config)# ipv6 prefix-list abc deny ::/0 ge 32
```

The following example denies all routes with a prefix of 2002::/128.

```
Router(config)# ipv6 prefix-list abc deny 2002::/128
```

The following example permits all routes with a prefix of ::/0.

```
Router(config)# ipv6 prefix-list abc permit ::/0
```

Related Commands

| Command | Description |
|---|--|
| clear ipv6 prefix-list | Resets the hit count of the IPv6 prefix list entries. |
| distribute-list out | Suppresses networks from being advertised in updates. |
| ipv6 prefix-list sequence-number | Enables the generation of sequence numbers for entries in an IPv6 prefix list. |
| match ipv6 address | Distributes IPv6 routes that have a prefix permitted by a prefix list. |
| show ipv6 prefix-list | Displays information about an IPv6 prefix list or IPv6 prefix list entries. |

ipv6 prefix-list sequence-number

To enable the generation of sequence numbers for entries in an IPv6 prefix list, use the **ipv6 prefix-list sequence-number** command in global configuration mode. To disable the generation of sequence numbers, use the **no** form of this command.

ipv6 prefix-list sequence-number

no ipv6 prefix-list sequence-number

Syntax Description This command has no arguments or keywords.

Defaults Sequence numbers are automatically generated for entries in an IPv6 prefix list.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines To suppress sequence numbers use the **no ipv6 prefix-list sequence-number** command. If you disable the generation of sequence numbers in an IPv6 prefix list, you must specify the sequence number for each entry using the *seq-number* argument of the **ipv6 prefix-list** command.

The **show ipv6 prefix-list** command displays the sequence numbers of entries.

Examples The following example shows the automatic sequence number generation for entries in an IPv6 prefix list being disabled:

```
Router(config)# no ipv6 prefix-list sequence-number
```

| Related Commands | Command | Description |
|------------------|------------------------------|---|
| | ipv6 prefix-list | Creates an entry in an IPv6 prefix list. |
| | show ipv6 prefix-list | Displays information about an IPv6 prefix list or IPv6 prefix list entries. |

ipv6 redirects

To enable the sending of Internet Control Message Protocol (ICMP) IPv6 redirect messages if Cisco IOS software is forced to resend a packet through the same interface on which the packet was received, use the **ipv6 redirects** command in interface configuration mode. To disable the sending of redirect messages, use the **no** form of this command.

ipv6 redirects

no ipv6 redirects

Syntax Description

This command has no arguments or keywords.

Defaults

The sending of ICMP IPv6 redirect messages is enabled.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(4)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The rate at which the router generates all IPv6 ICMP error messages can be limited by using the **ipv6 icmp error-interval** command.

Examples

The following example disables the sending of ICMP IPv6 redirect messages on Ethernet interface 0 and reenables the messages on Ethernet interface 1:

```
Router(config)# interface ethernet 0
Router(config-if)# no ipv6 redirects
```

```
Router(config)# interface ethernet 1
Router(config-if)# ipv6 redirects
```

To verify whether the sending of IPv6 redirect messages is enabled or disabled on an interface, enter the **show ipv6 interface EXEC** command:

```
Router# show ipv6 interface
```

```
Ethernet0 is up, line protocol is up
  IPv6 is stalled, link-local address is FE80::1
  Global unicast address(es):
    2000::1, subnet is 2000::/64
    3000::1, subnet is 3000::/64
  Joined group address(es):
```



```

FF02::1
FF02::2
FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are disabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.

Ethernet1 is up, line protocol is up
IPv6 is stalled, link-local address is FE80::2
Global unicast address(es):
  2000::2, subnet is 2000::/64
  3000::3, subnet is 3000::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is disabled, number of DAD attempts: 0
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.

```

Related Commands

| Command | Description |
|---------------------------------|---|
| ipv6 icmp error-interval | Configures the interval for IPv6 ICMP error messages. |

ipv6 rip default-information

To originate a default IPv6 route into the Routing Information Protocol (RIP), use the **ipv6 rip default-information** command in interface configuration mode. To remove the default IPv6 RIP route, use the **no** form of this command.

ipv6 rip *word* **default-information** { **only** | **originate** }

no ipv6 rip *word* **default-information**

Syntax Description

| | |
|------------------|--|
| <i>word</i> | Name of the IPv6 RIP routing process. |
| only | Advertises the IPv6 default route (::/0) only. Suppresses the advertisement of all other routes. |
| originate | Advertises the IPv6 default route (::/0). The advertisement of other routes is unaffected. |

Defaults

Disabled

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **ipv6 rip default-information** command is similar to the **default-information originate** (RIP) command, except that it is IPv6-specific.

Originating a default IPv6 route into RIP also forces the advertisement of the route in router updates sent on the interface. The advertisement of the route occurs regardless of whether the route is present in the IPv6 routing table.



Note

To avoid routing loops after the IPv6 default route (::/0) is originated into a specified RIP routing process, the routing process ignores all default route information received in subsequent IPv6 RIP update messages.

Examples

The following example originates a default IPv6 route into RIP on Ethernet interface 0/0 and advertises only the default route in router updates sent on the interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 rip cisco default-information only
```

The following example originates a default IPv6 route into RIP on Ethernet interface 0/0 and advertises the default route with all other routes in router updates sent on the interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 rip cisco default-information originate
```

Related Commands

| Command | Description |
|----------------------|--|
| show ipv6 rip | Displays information about current IPv6 RIP processes. |

ipv6 rip enable

To enable an IPv6 Routing Information Protocol (RIP) routing process on an interface, use the **ipv6 rip enable** command in interface configuration mode. To disable an IPv6 RIP routing process on an interface, use the **no** form of this command.

ipv6 rip *word* **enable**

no ipv6 rip *word*

Syntax Description

| | |
|-------------|---------------------------------------|
| <i>word</i> | Name of the IPv6 RIP routing process. |
|-------------|---------------------------------------|

Defaults

An IPv6 RIP routing process is not defined.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **ipv6 rip enable** interface configuration command is used to enable IPv6 RIP explicitly on required interfaces. In IPv4, the **network** *network-number* router configuration command is used to implicitly specify the interfaces on which to run IPv4 RIP.

Examples

The following example enables the IPv6 RIP routing process named cisco on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 rip cisco enable
```

Related Commands

| Command | Description |
|----------------------|--|
| show ipv6 rip | Displays information about current IPv6 RIP processes. |

ipv6 rip metric-offset

To set the IPv6 Routing Information Protocol (RIP) metric for an interface, use the **ipv6 rip metric-offset** command in interface configuration mode. To return the metric to its default value, use the **no** form of this command.

ipv6 rip *word* **metric-offset** *value*

no ipv6 rip *word* **metric-offset**

Syntax Description

| | |
|--------------|---|
| <i>word</i> | Name of the IPv6 RIP routing process. |
| <i>value</i> | Value added to the metric of an IPv6 RIP route received in a report message. A number from 1 to 16. |

Defaults

The default metric value is 1.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

When an IPv6 RIP route is received, the interface metric value set by the **ipv6 rip metric-offset** command is added before the route is inserted into the routing table. Therefore, increasing the IPv6 RIP metric value of an interface increases the metric value of IPv6 RIP routes received over the interface.

Use the **ipv6 rip metric-offset** command to influence which routes are used, as you prefer. The IPv6 RIP metric is in hop count.

Examples

The following example configures a metric increment of 10 for the RIP routing process named cisco on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 rip cisco metric-offset 10
```

Related Commands

| Command | Description |
|----------------------|--|
| show ipv6 rip | Displays information about current IPv6 RIP processes. |

ipv6 rip summary-address

To configure IPv6 Routing Information Protocol (RIP) to advertise summarized IPv6 addresses on an interface and to specify the IPv6 prefix that identifies the routes to be summarized, use the **ipv6 rip summary-address** command in interface configuration mode. To stop the advertising of the summarized IPv6 addresses, use the **no** form of this command.

ipv6 rip *word* **summary-address** *ipv6-prefix/prefix-length*

no ipv6 rip *word* **summary-address**

Syntax Description

| | |
|-----------------------|--|
| <i>word</i> | Name of the IPv6 RIP routing process. |
| <i>ipv6-prefix</i> | Specifies an IPv6 network number as the summary address. 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> | The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **ipv6 rip summary-address** command is similar to the **ip summary-address rip** command, except that it is IPv6-specific.

Use the **ipv6 rip summary-address** command to force IPv6 RIP to advertise specific networks on specific interfaces (assuming that routes to those networks exist).

If the first bits of the prefix length for a route match the value specified for the *ipv6-prefix* argument, the prefix specified in the *ipv6-prefix* argument is advertised instead of the route. As a result, multiple routes can be replaced by a single route whose metric is the lowest metric of the multiple routes.

Examples

In the following example, the IPv6 address 2001:0DB8:0:1:260:3EFF:FE11:6770 that is assigned to Ethernet interface 0/0 with an IPv6 prefix length of 64 bits is summarized as IPv6 prefix 2001:0DB8::/35 for the IPv6 RIP routing process named cisco:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 address 2001:0DB8:0:1:260:3EFF:FE11:6770 /64
Router(config-if)# ipv6 rip cisco summary-address 2001:0DB8::/35
```



Note

A route advertisement that is suppressed as a result of split horizon is not considered by RIP when RIP is deciding whether to advertise a summary route.

Related Commands

| Command | Description |
|----------------------------------|--|
| poison-reverse (IPv6 RIP) | Configures the poison reverse processing of IPv6 RIP router updates. |
| show ipv6 rip | Displays information about current IPv6 RIP processes. |

ipv6 route

To establish static IPv6 routes, use the **ipv6 route** command in global configuration mode. To remove a previously configured static route, use the **no** form of this command.

ipv6 route *ipv6-prefix/prefix-length* { *ipv6-address* | *interface-type interface-number* [*ipv6-address*] } [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**]

no ipv6 route *ipv6-prefix/prefix-length* { *ipv6-address* | *interface-type interface-number* [*ipv6-address*] } [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**]

Syntax Description

| | |
|--------------------------------|--|
| <i>ipv6-prefix</i> | The IPv6 network that is the destination of the static route. Can also be a host name when static host routes are configured. |
| <i>/prefix-length</i> | The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |
| <i>ipv6-address</i> | <p>The IPv6 address of the next hop that can be used to reach the specified network. The IPv6 address of the next hop need not be directly connected; recursion is done to find the IPv6 address of the directly connected next hop.</p> <p>When an interface type and interface number are specified, you can optionally specify the IPv6 address of the next hop to which packets are output.</p> <p>Note You must specify an interface type and an interface number when using a link-local address as the next hop (the link-local next hop must also be an adjacent router).</p> <p>This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</p> |
| <i>interface-type</i> | <p>Interface type. For more information about supported interface types, use the question mark (?) online help function.</p> <p>You can use the <i>interface-type</i> argument to direct static routes out point-to-point interfaces (such as serial or tunnel interfaces) and broadcast interfaces (such as Ethernet interfaces). When using the <i>interface-type</i> argument with point-to-point interfaces, there is no need to specify the IPv6 address of the next hop. When using the <i>interface-type</i> argument with broadcast interfaces, you should always specify the IPv6 address of the next hop or ensure that the specified prefix is assigned to the link. A link-local address should be specified as the next hop for broadcast interfaces.</p> |
| <i>interface-number</i> | Interface number. For more information about the numbering syntax for supported interface types, use the question mark (?) online help function. |
| <i>administrative-distance</i> | (Optional) An administrative distance. The default value is 1, which gives static routes precedence over any other type of route except connected routes. |

| | |
|--|--|
| <i>administrative-multicast-distance</i> | (Optional) The distance used when selecting this route for multicast reverse path forwarding (RPF). |
| unicast | (Optional) Specifies a route that must not be used in multicast RPF selection. |
| multicast | (Optional) Specifies a route that must not be populated in the unicast routing information base (RIB). |

Defaults

No static routes are established.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|---|
| 12.2(2)T | This command was introduced. |
| 12.2(4)T | The optional <i>ipv6-address</i> argument was added. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.0(26)S | The optional unicast and multicast keywords and <i>administrative-multicast-distance options</i> argument were added. |
| 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines

Use the **ipv6 route** command to implement static multicast routes in IPv6. For a static multicast route, the IPv6 address of the next-hop router must be provided. The *administrative-multicast-distance* argument determines the distance that will be used when selecting this route for RPF. When the **unicast** keyword is used, this route will not be used in multicast RPF selection.

When the **ipv6 route** command is used with the **multicast** keyword, the route will not be populated in the unicast RIB. When the optional *administrative-multicast-distance* argument is not specified, the multicast RPF administrative distance defaults to the same value as that determined by the *administrative-distance* argument.

Examples

The following example shows a static route that applies to unicast routing only:

```
ipv6 route 2001::/64 5::5 100 unicast
```

The following example shows a static route used only for multicast RPF selection:

```
ipv6 route 2001::/64 7::7 100 multicast
```

The following example shows a static route used for both unicast routing and multicast RPF selection:

```
ipv6 route 2001::/64 6::6 100
```

The following example shows a static route used for both unicast routing and multicast RPF selection, but with different administrative distances:

```
ipv6 route 10::/64 7::7 100 200
```

Related Commands

| Command | Description |
|-------------------------|--|
| show ipv6 route | Displays the current contents of the IPv6 routing table. |
| show ipv6 route summary | Displays the current contents of the IPv6 routing table in summary format. |
| show ipv6 rpf | Checks RPF information for a given unicast host address and prefix. |

ipv6 router isis

To configure an Intermediate System-to-Intermediate System (IS-IS) routing process for IPv6 on an interface and to attach an area designator to the routing process, use the **ipv6 router isis** command in interface configuration mode. To disable IS-IS for IPv6, use the **no** form of the command.

ipv6 router isis *area-name*

no ipv6 router isis *area-name*

Syntax Description

| | |
|------------------|--|
| <i>area-name</i> | Meaningful name for a routing process. If a name is not specified, a null name is assumed and the process is referenced with a null name. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. Required for multiarea IS-IS configuration. Each area in a multiarea configuration should have a nonnull area name to facilitate identification of the area. Optional for conventional IS-IS configuration. |
|------------------|--|

Defaults

No routing processes are specified.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(8)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

Before the IPv6 IS-IS routing process can be configured, IPv6 routing must be enabled using the **ipv6 unicast-routing** global configuration command, and an IPv6 address must be configured on an interface using either the **ipv6 enable** interface configuration command or the **ipv6 address** interface configuration command. The **ipv6 enable** command will automatically configure an IPv6 link-local address on the interface.

Examples

The following example specifies IS-IS as an IPv6 routing protocol for a process named Finance. The Finance process will run over the Fast Ethernet interface 0/1.

```
Router(config)# router isis Finance
Router(config-router)# net 49.0001.aaaa.aaaa.aaaa.00
Router(config-router)# exit
Router(config)# interface FastEthernet 0/1
Router(config-if)# ipv6 router isis Finance
```

Related Commands

| Command | Description |
|--------------------------------|---|
| ipv6 address link-local | Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface. |
| ipv6 enable | Enables an interface for IPv6 processing and automatically assigns an IPv6 link-local address on the interface. |
| ipv6 unicast-routing | Enables the forwarding of IPv6 unicast datagrams. |
| net | Configures an IS-IS NET for a CLNS routing process. |
| router isis | Enables the IPv4 IS-IS routing protocol. |

ipv6 router ospf

To enable OSPF router configuration mode, use the **ipv6 router ospf** command in global configuration mode.

ipv6 router ospf

Syntax Description This command has no arguments or keywords.

Defaults No OSPF routing process is defined.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines Use this command to enter the OSPF router configuration mode. From this mode, you can enter several commands to customize OSPF for IPv6.

Examples The following example enables router OSPF configuration mode:

```

ipv6 router ospf

```

ipv6 router rip

To configure an IPv6 Routing Information Protocol (RIP) routing process, use the **ipv6 router rip** command in global configuration mode. To remove a routing process, use the **no** form of this command.

```
ipv6 router rip word

no ipv6 router rip word
```

| | | |
|--------------------|------|--|
| Syntax Description | word | A word that describes the routing process. |
|--------------------|------|--|

| | |
|----------|---|
| Defaults | No IPv6 RIP routing process is defined. |
|----------|---|

| | |
|---------------|----------------------|
| Command Modes | Global configuration |
|---------------|----------------------|

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

| | |
|------------------|---|
| Usage Guidelines | The ipv6 router rip command is similar to the router rip command, except that it is IPv6-specific. |
| | Use this command to enable an IPv6 RIP routing process. Configuring this command places the router in router configuration mode for the IPv6 RIP routing process. The router prompt changes to Router(config-rtr-rip)#. |

| | |
|----------|--|
| Examples | The following example configures the IPv6 RIP routing process named cisco and places the router in router configuration mode for the IPv6 RIP routing process: Router(config)# ipv6 router rip cisco |
|----------|--|

| Related Commands | Command | Description |
|------------------|------------------------|--|
| | ipv6 rip enable | Enables an IPv6 RIP routing process on an interface. |

ipv6 traffic-filter

To filter incoming or outgoing IPv6 traffic on an interface, use the **ipv6 traffic-filter** command in interface configuration mode. To disable the filtering of IPv6 traffic on an interface, use the **no** form of this command.

ipv6 traffic-filter *access-list-name* {**in** | **out**}

no ipv6 traffic-filter *access-list-name*

Syntax Description

| | |
|-------------------------|----------------------------------|
| <i>access-list-name</i> | Specifies an IPv6 access name. |
| in | Specifies incoming IPv6 traffic. |
| out | Specifies outgoing IPv6 traffic. |

Defaults

Filtering of IPv6 traffic on an interface is not configured.

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Examples

The following example filters inbound IPv6 traffic on Ethernet interface 0/0 as defined by the access list named cisco:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 traffic-filter cisco in
```

Related Commands

| Command | Description |
|------------------------------|---|
| ipv6 access-list | Defines an IPv6 access list and sets deny or permit conditions for the defined access list. |
| show ipv6 access-list | Displays the contents of all current IPv6 access lists. |
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 unicast-routing

To enable the forwarding of IPv6 unicast datagrams, use the **ipv6 unicast-routing** command in global configuration mode. To disable the forwarding of IPv6 unicast datagrams, use the **no** form of this command.

ipv6 unicast-routing

no ipv6 unicast-routing

Syntax Description This command has no arguments or keywords.

Defaults IPv6 unicast routing is disabled.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines Configuring the **no ipv6 unicast-routing** command removes all IPv6 routing protocol entries from the IPv6 routing table.

Examples The following example enables the forwarding of IPv6 unicast datagrams:

```
Router(config)# ipv6 unicast-routing
```

| Related Commands | Command | Description |
|------------------|--------------------------------|--|
| | ipv6 address link-local | Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface. |
| | ipv6 address eui-64 | Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address. |
| | ipv6 enable | Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address. |
| | ipv6 unnumbered | Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface. |
| | show ipv6 route | Displays the current contents of the IPv6 routing table. |

ipv6 unnumbered

To enable IPv6 processing on an interface without assigning an explicit IPv6 address to the interface, use the **ipv6 unnumbered** command in interface configuration mode. To disable IPv6 on an unnumbered interface, use the **no** form of this command.

ipv6 unnumbered *interface-type interface-number*

no ipv6 unnumbered

Syntax Description

| | |
|-------------------------|--|
| <i>interface-type</i> | The interface type of the source address that the unnumbered interface uses in the IPv6 packets that it originates. The source address cannot be another unnumbered interface. |
| <i>interface-number</i> | The interface number of the source address that the unnumbered interface uses in the IPv6 packets that it originates. |

Defaults

Disabled

Command Modes

Interface configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **ipv6 unnumbered** command is similar to the **ip unnumbered** command, except that it is IPv6-specific.

IPv6 packets that are originated from an unnumbered interface use the global IPv6 address of the interface specified in the **ipv6 unnumbered** command as the source address for the packets.



Note

Serial interfaces using High-Level Data Link Control (HDLC), PPP, Link Access Procedure, Balanced (LAPB), Frame Relay encapsulations, and tunnel interfaces can be unnumbered. You cannot use this interface configuration command with X.25 or Switched Multimegabit Data Service (SMDS) interfaces.

The interface you specify with the *interface-type* and *interface-number* arguments must be enabled (listed as “up” in the **show ipv6 interface** command display).

Examples

The following example configures serial interface 0/1 as unnumbered. IPv6 packets that are sent on serial interface 0/1 use the IPv6 address of Ethernet 0/0 as their source address:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 address 3FFE:C00:0:1:260:3EFF:FE11:6770

Router(config)# interface serial 0/1
Router(config-if)# ipv6 unnumbered ethernet 0/0
```

Related Commands

| Command | Description |
|----------------------------|--|
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |

ipv6 verify unicast reverse-path

To enable Unicast Reverse Path Forwarding (Unicast RPF) for IPv6, use the **ipv6 verify unicast reverse-path** interface configuration command. To disable Unicast RPF, use the **no** form of this command.

ipv6 verify unicast reverse-path [*access-list name*]

no ipv6 verify unicast reverse-path [*access-list name*]

| | | |
|---------------------------|---|---|
| Syntax Description | access-list name (Optional) Specifies the name of the access list. | |
| Defaults | Unicast RPF is disabled. | |
| Command Modes | Interface configuration | |
| Command History | Release | Modification |
| | 12.2(13)T | This command was introduced. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| Usage Guidelines | <p>Use the ipv6 verify unicast reverse-path interface command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IP address spoofing.</p> <p>When Unicast RPF is enabled on an interface, the router examines all packets received on that interface. The router checks to make sure that the source address appears in the routing table and matches the interface on which the packet was received. Unicast RPF is an input feature and is applied only on the input interface of a router at the upstream end of a connection.</p> <p>The Unicast Reverse Path Forwarding feature performs a reverse lookup in the CEF table to see if any packet received at a router interface has arrived on a path identified as a best return paths to the source of the packet. The feature does this by performing a reverse lookup in the CEF table. If Unicast RPF does not find a reverse path for the packet, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast Reverse Path Forwarding command. If an ACL is specified in the command, then when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.</p> <p>If no ACL is specified in the Unicast Reverse Path Forwarding command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.</p> <p>Unicast RPF events can be logged by specifying the logging option for the ACL entries used by the Unicast Reverse Path Forwarding command. Log information can be used to gather information about the attack, such as source address, time, and so on.</p> | |


Note

When using Unicast RPF, all equal-cost “best” return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on).

Unicast RPF should not be used on interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry, meaning that there are multiple routes to the source of a packet. Unicast RPF should be applied only where there is natural or configured symmetry.

For example, routers at the edge of the network of an Internet service provider (ISP) are more likely to have symmetrical reverse paths than routers that are in the core of the ISP network. Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router. Hence, it is not recommended that you apply Unicast RPF where there is a chance of asymmetric routing. It is simplest to place Unicast RPF only at the edge of a network or, for an ISP, at the customer edge of the network.

Examples
Unicast Reverse Path Forwarding on a Serial Interface Example

The following example shows enabling the Unicast Reverse Path Forwarding feature on a serial interface:

```
interface serial 5/0/0
  ipv6 verify unicast reverse-path
```

Single-homed ISP Example

The following example uses a very simple single-homed ISP to demonstrate the concepts of ingress and egress filters used in conjunction with Unicast RPF. The example illustrates an ISP-allocated classless interdomain routing (CIDR) block 209.165.202.128/28 that has both inbound and outbound filters on the upstream interface. Be aware that ISPs are usually not single-homed. Hence, provisions for asymmetrical flows (when outbound traffic goes out one link and returns via a different link) need to be designed into the filters on the border routers of the ISP.

```
interface Serial 5/0/0
  description Connection to Upstream ISP
  ipv6 address FE80::260:3EFF:FE11:6770/64
  no ipv6 redirects
  ipv6 verify unicast reverse-path abc
  !
  ipv6 access-list abc
  permit ipv6 host 2::1 any
  deny ipv6 FEC0::/10 any
  ipv6 access-group abc in
  ip access-group jkl out
  !
  access-list abc permit ip FE80::260:3EFF:FE11:6770/64 2001:0DB8:0000:0001::0001 any
  access-list abc deny ipv6 any any log
  access-list jkl deny ipv6 host 2001:0DB8:0000:0001::0001 any log
  access-list jkl deny ipv6 2001:0DB8:0000:0001:FFFF:1234::5 255.255.255 any log
  access-list jkl deny ipv6 2002:0EF8:002001:0DB8:0000:0001:FFFF:1234::5 172.16.0.0
    15.255.255 any log
  access-list jkl deny ipv6 2001:0CB8:0000:0001:FFFF:1234::5 0.0.255.255 any log
  access-list jkl deny ipv6 2003:0DB8:0000:0001:FFFF:1234::5 0.0.0.31 any log
  access-list jkl permit ipv6
```

ACL Logging with Unicast RPF Example

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL abc provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet0/0 to check packets arriving at that interface.

For example, packets with a source address of 8765:4321::1 arriving at interface Ethernet0 are dropped because of the deny statement in ACL 'abc'. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 1234:5678::1 arriving at interface Ethernet0/0 are forwarded because of the permit statement in ACL abc. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
!
interface ethernet 0/0
  ipv6 address FE80::260:3EFF:FE11:6770/64 link-local
  ipv6 verify unicast reverse-path abc
!
ipv6 access-list abc
  permit ipv6 1234:5678::/64 any log-input
  deny ipv6 8765:4321::/64 any log-input
!
```

Related Commands

| Command | Description |
|-----------------|--|
| ip cef | Enables CEF on the route processor card. |
| ipv6 cef | enables CEF for IPv6 interfaces. |

isis ipv6 metric

To configure the value of an Intermediate System-to-Intermediate System (IS-IS) IPv6 metric, use the **isis ipv6 metric** command in interface configuration mode. To return the metric to its default value, use the **no** form of this command.

isis ipv6 metric *metric-value* [**level-1** | **level-2** | **level-1-2**]

no isis ipv6 metric *metric-value* [**level-1** | **level-2** | **level-1-2**]

Syntax Description

| | |
|---------------------|---|
| <i>metric-value</i> | Value added to the metric of an IPv6 IS-IS route received in a report message. The default metric value is 10. The range is from 1 to 16777214. |
| level-1 | (Optional) Enables this command on routing Level 1. |
| level-2 | (Optional) Enables this command on routing Level 2. |
| level-1-2 | (Optional) Enables this command on routing Levels 1 and 2. |

Defaults

The default metric value is 10.

Command Modes

Interface configuration

Command History

| Release | Modification |
|-----------|---|
| 12.2(15)T | This command was introduced. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

The **isis ipv6 metric** command is used only in multitopology IS-IS.

Changing the metric allows differentiation between IPv4 and IPv6 traffic, forcing traffic onto different interfaces. This function allows you to use the lower-cost rather than the high-cost interface.

For using extended metrics, such as with the IS-IS multitopology for IPv6 feature, Cisco IOS software provides support of a 24-bit metric field, the so-called “wide metric.” Using the new metric style, link metrics now have a maximum value of 16777214 with a total path metric of 4261412864.

Examples

The following example sets the value of an IS-IS IPv6 metric to 20:

```
Router(config)# interface Ethernet 0/0/1
Router(config-if)# isis ipv6 metric 20
```

match dscp

To identify a specific IP differentiated service code point (DSCP) value as a match criterion, use the **match dscp** class-map configuration command. To remove a specific DSCP value from a class map, use the **no** form of this command.

match [ip] dscp *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*]

no match [ip] dscp *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*]

| | | |
|---------------------------|-------------------|--|
| Syntax Description | ip | (Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets. |
| | <i>dscp-value</i> | Specifies the exact value from 0 to 63 used to identify an IP DSCP value. |

Defaults Matching occurs on both IPv4 and IPv6 packets.

Command Modes Class-map configuration

| Command History | Release | Modification |
|------------------------|----------------|--|
| | 12.2(13)T | This command was introduced. This command replaces the match ip dscp command. |

Usage Guidelines

DSCP Values

Up to eight DSCP values can be matched in one match statement. For example, if you wanted the DSCP values of 0, 1, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values must be a successful match criterion, not all of the specified DSCP values), enter the **match dscp 0 1 2 3 4 5 6 7** command.

This command is used by the class map to identify a specific DSCP value marking on a packet. In this context, *dscp-value* arguments are used as markings only and have no mathematical significance. For instance, the *dscp-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *dscp-value* of 2 is different than a packet marked with the *dscp-value* of 1. The treatment of these marked packets is defined by the user through the setting of QoS policies in policy-map class configuration mode.

Match IPv6 Packets on DSCP Values

To match DSCP values for IPv6 packets only, the **match protocol ipv6** command must also be used. Without that command, the DSCP match defaults to match both IPv4 and IPv6 packets.

Match IPv4 Packets on DSCP Values

To match DSCP values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword the match occurs on both IPv4 and IPv6 packets. Alternatively, the **match protocol ip** command can be used with **match dscp** to classify only IPv4 packets.

Examples

Priority50 Service Policy Matching DSCP Value

The following example shows how to configure the service policy called priority50 and attach service policy priority50 to an interface. In this example, the class map called ipdscp15 will evaluate all packets entering interface Fast Ethernet 1/0/0 for an IP DSCP value of 15. If the incoming packet has been marked with the IP DSCP value of 15, the packet will be treated as priority traffic and will be allocated with bandwidth of 50 kbps.

```
Router(config)# class-map ipdscp15
Router(config-cmap)# match ip dscp 15
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipdscp15
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy output priority50
```

Related Commands

| Command | Description |
|-----------------------|---|
| class-map | Creates a class map to be used for matching packets to a specified class. |
| policy-map | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| service-policy | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| set dscp | Marks the DSCP value for packets within a traffic class. |
| show class-map | Displays all class maps and their matching criteria. |

match ipv6 address

To distribute IPv6 routes that have a prefix permitted by a prefix list, use the **match ipv6 address** command in route-map configuration mode. To remove the **match ipv6 address** entry, use the **no** form of this command.

match ipv6 address {**prefix-list** *prefix-list-name*}

no match ipv6 address

Syntax Description

prefix-list *prefix-list-name* Name of an IPv6 prefix list.

Defaults

No routes are distributed based on destination network number.

Command Modes

Route-map configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **match ipv6 address** command is similar to the **match ip address** command, except that it is IPv6-specific.

Use the **route-map** command, and the **match** and **set** commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** command has multiple formats. The **match** commands can be given in any order, and all **match** commands must “pass” to cause the route to be redistributed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

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



Note

A permit route map containing only **set** commands and no **match** commands permits all routes.

Examples

In the following example, IPv6 routes that have addresses specified by the prefix list named marketing are matched:

```
Router(config)# route-map name
Router(config-route-map)# match ipv6 address prefix-list marketing
```

Related Commands

| Command | Description |
|--------------------------------|--|
| match as-path | Matches a BGP autonomous system path access list. |
| match community | Matches a BGP community. |
| match ipv6 next-hop | Distributes IPv6 routes that have a next hop prefix permitted by a prefix list. |
| match ipv6 route-source | Distributes IPv6 routes that have been advertised by routers at an address specified by a prefix list. |
| match metric | Redistributes routes with the metric specified. |
| match route-type | Redistributes routes of the specified type. |
| route-map | Defines the conditions for redistributing routes from one routing protocol into another. |
| set as-path | Modifies an autonomous system path for BGP routes. |
| set community | Sets the BGP community attribute. |
| set level | Indicates where to import routes. |
| set local preference | Specifies a preference value for the autonomous system path. |
| set metric | Sets the metric value for a routing protocol. |
| set metric-type | Sets the metric type for the destination routing protocol. |
| set tag | Sets a tag value of the destination routing protocol. |
| set weight | Specifies the BGP weight for the routing table. |

match ipv6 next-hop

To distribute IPv6 routes that have a next hop prefix permitted by a prefix list, use the **match ipv6 next-hop** command in route-map configuration mode. To remove the **match ipv6 next-hop** entry, use the **no** form of this command.

match ipv6 next-hop {**prefix-list** *prefix-list-name*}

no match ipv6 next-hop

Syntax Description

prefix-list *prefix-list-name* Name of an IPv6 prefix list.

Defaults

Routes are distributed freely, without being required to match a next hop address.

Command Modes

Route-map configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **match ipv6 next-hop** command is similar to the **match ip next-hop** command, except that it is IPv6-specific.

Use the **route-map** command, and the **match** and **set** commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** command has multiple formats. The **match** commands can be given in any order, and all **match** commands must “pass” to cause the route to be redistributed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

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



Note

A permit route map containing only **set** commands and no **match** commands permits all routes.

Examples

The following example distributes routes that have a next hop IPv6 address passed by the prefix list named marketing:

```
Router(config)# route-map name
Router(config-route-map)# match ipv6 next-hop prefix-list marketing
```

Related Commands

| Command | Description |
|--------------------------------|--|
| match as-path | Matches a BGP autonomous system path access list. |
| match community | Matches a BGP community. |
| match ipv6 address | Distributes IPv6 routes that have a prefix permitted by a prefix list. |
| match ipv6 route-source | Distributes IPv6 routes that have been advertised by routers at an address specified by a prefix list. |
| match metric | Redistributes routes with the metric specified. |
| match route-type | Redistributes routes of the specified type. |
| route-map | Defines the conditions for redistributing routes from one routing protocol into another. |
| set as-path | Modifies an autonomous system path for BGP routes. |
| set community | Sets the BGP community attribute. |
| set level | Indicates where to import routes. |
| set local preference | Specifies a preference value for the autonomous system path. |
| set metric | Sets the metric value for a routing protocol. |
| set metric-type | Sets the metric type for the destination routing protocol. |
| set tag | Sets a tag value of the destination routing protocol. |
| set weight | Specifies the BGP weight for the routing table. |

match ipv6 route-source

To distribute IPv6 routes that have been advertised by routers at an address specified by a prefix list, use the **match ipv6 route-source** command in route-map configuration mode. To remove the **match ipv6 route-source** entry, use the **no** form of this command.

```
match ipv6 route-source {prefix-list prefix-list-name}
```

```
no match ipv6 route-source
```

Syntax Description

| | |
|--|------------------------------|
| prefix-list <i>prefix-list-name</i> | Name of an IPv6 prefix list. |
|--|------------------------------|

Defaults

No filtering on route source.

Command Modes

Route-map configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **match ipv6 route-source** command is similar to the **match ip route-source** command, except that it is IPv6-specific.

Use the **route-map** command, and the **match** and **set** commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** command has multiple formats. The **match** commands can be given in any order, and all **match** commands must “pass” to cause the route to be redistributed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

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

There are situations in which the next hop for a route and the source networking device address are not the same.

**Note**

A permit route map containing only **set** commands and no **match** commands permits all routes.

Examples

The following example distributes routes that have been advertised by networking devices at the addresses specified by the prefix list named marketing:

```
Router(config)# route-map name
Router(config-route-map)# match ipv6 route-source prefix-list marketing
```

Related Commands

| Command | Description |
|-----------------------------|--|
| match as-path | Matches a BGP autonomous system path access list. |
| match community | Matches a BGP community. |
| match ipv6 address | Distributes IPv6 routes that have a prefix permitted by a prefix list. |
| match ipv6 next-hop | Distributes IPv6 routes that have a next hop prefix permitted by a prefix list. |
| match metric | Redistributes routes with the metric specified. |
| match route-type | Redistributes routes of the specified type. |
| route-map | Defines the conditions for redistributing routes from one routing protocol into another. |
| set as-path | Modifies an autonomous system path for BGP routes. |
| set community | Sets the BGP community attribute. |
| set level | Indicates where to import routes. |
| set local preference | Specifies a preference value for the autonomous system path. |
| set metric | Sets the metric value for a routing protocol. |
| set metric-type | Sets the metric type for the destination routing protocol. |
| set tag | Sets a tag value of the destination routing protocol. |
| set weight | Specifies the BGP weight for the routing table. |

match precedence

To identify IP precedence values as match criteria, use the **match precedence** command in class-map configuration mode. To remove IP precedence values from a class map, use the **no** form of this command.

match [ip] precedence precedence-value [precedence-value precedence-value precedence-value]

no match [ip] precedence precedence value [precedence-value precedence-value precedence-value]

| | | |
|---------------------------|-------------------------|--|
| Syntax Description | ip | (Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IP and IPv6 packets. |
| | <i>precedence-value</i> | Specifies the exact value from 0 to 7 used to identify a precedence value. |

Defaults Matching on both IPv4 and IPv6 packets is the default.

Command Modes Class-map configuration

| Command History | Release | Modification |
|------------------------|----------------|--|
| | 12.2(13)T | This command was introduced. This command replaces the match ip precedence command. |

Usage Guidelines

Precedence Value Arguments

Up to four precedence values can be matched in one match statement. For example, if you wanted the precedence values of 0, 1, 2, or 3 (note that only one of the precedence values must be a successful match criterion, not all of the specified precedence values), enter the **match ip precedence 0 1 2 3** command.

The *precedence-value* arguments are used as markings only. In this context, the IP precedence values have no mathematical significance. For instance, the *precedence-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *precedence-value* of 2 is different than a packet marked with the *precedence-value* of 1. The treatment of these different packets is defined by the user through the setting of QoS policies in policy-map class configuration mode.

Match on Precedence for IPv6 Only

To match on precedence values for IPv6 packets only, the **match protocol ipv6** command must also be used. Without that command, the precedence match defaults to match both IPv4 and IPv6 packets.

Match on Precedence for IPv4 Packets Only

To match on precedence values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword the match occurs on both IPv4 and IPv6 packets.

Examples

IPv4-Specific Traffic Match

The following example shows how to configure the service policy called priority50 and attach service policy priority50 to an interface, matching for IPv4 traffic only. In a network where both IPv4 and IPv6 are running, you might find it necessary to distinguish between the protocols for matching and traffic segregation. In this example, the class map called ipprec5 will evaluate all IPv4 packets entering Fast Ethernet interface 1/0/0 for a precedence value of 5. If the incoming IPv4 packet has been marked with the precedence value of 5, the packet will be treated as priority traffic and will be allocated with bandwidth of 50 kbps.

```
Router(config)# class-map ipprec5
Router(config-cmap)# match ip precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority50
```

IPv6-Specific Traffic Match

The following example shows the same service policy matching on precedence for IPv6 traffic only. Notice that the **match protocol** command with the **ipv6** keyword precedes the **match precedence** command. The **match protocol** command is required to perform matches on IPv6 traffic alone.

```
Router(config)# class-map ipprec5
Router(config-cmap)# match protocol ipv6
Router(config-cmap)# match precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority50
```

Related Commands

| Command | Description |
|--------------------------|---|
| class-map | Creates a class map to be used for matching packets to a specified class. |
| match protocol | Configures the match criteria for a class map on the basis of a specified protocol. |
| policy-map | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| service-policy | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| set ip precedence | Sets the precedence value in the IP header. |
| show class-map | Displays all class maps and their matching criteria, or a specified class map and its matching criteria. |

match protocol

To configure the match criteria for a class map on the basis of the specified protocol, use the **match protocol** class-map configuration command. To remove protocol-based match criteria from a class map, use the **no** form of this command.

match protocol *protocol-name*

no match protocol *protocol-name*

| Syntax Description | <i>protocol-name</i> | <p>Name of the protocol used as a matching criterion. Supported protocols include the following:</p> <ul style="list-style-type: none"> • aarp—AppleTalk Address Resolution Protocol • apollo—Apollo Domain • arp—IP Address Resolution Protocol (ARP) • bridge—bridging • bstun—Block Serial Tunneling • cdp—Cisco Discovery Protocol • clns—ISO Connectionless Network Service • clns_es—ISO CLNS End System • clns_is—ISO CLNS Intermediate System • cmns—ISO Connection-Mode Network Service • compressedtcp—compressed TCP • decnet—DECnet • decnet_node—DECnet Node • decnet_router-I1—DECnet Router L1 • decnet_router-I2—DECnet Router L2 • dls—data-link switching • ip—IP • ipv6—IPv6 • ipx—Novell IPX • llc2—llc2 • pad—packet assembler/disassembler links • qlc—Qualified Logical Link Control protocol • rsrb—remote source-route bridging • snapshot—snapshot routing support • stun—serial tunnel • vines—Banyan VINES • xns—Xerox Network Services |
|--------------------|----------------------|---|
|--------------------|----------------------|---|

Defaults

This command has no default behavior or values.

Command Modes

Class-map configuration

Command History

| Release | Modification |
|-----------|---|
| 12.0(5)T | This command was introduced. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE. |
| 12.0(7)S | This command was integrated into Cisco IOS Release 12.0(7)S. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.2(13)T | The ipv6 keyword was added to support protocol matching on IPv6 packets. |

Usage Guidelines

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria including protocols, access control lists (ACLs), input interfaces, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match protocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

To use the **match protocol** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

This command can be used to match protocols that are known to the Network-Based Application Recognition (NBAR) feature. For a list of protocols currently supported by NBAR, see the “Classification” section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

The following example specifies a class map called ipx and configures the Internetwork Packet Exchange (IPX) protocol as a match criterion for it:

```
class-map ipx
  match protocol ipx
```

The following example configures NBAR to match File Transfer Protocol (FTP) traffic:

```
match protocol ftp
```

Related Commands

| Command | Description |
|------------------------------|---|
| class-map | Creates a class map to be used for matching packets to a specified class. |
| match access-group | Configures the match criteria for a class map based on the specified ACL. |
| match input-interface | Configures a class map to use the specified input interface as a match criterion. |
| match precedence | Identifies IP precedence values as match criteria. |
| match qos-group | Configures a class map to use the specified EXP field value as a match criterion. |

maximum-paths (IPv6)

To control the maximum number of equal-cost routes that an IPv6 Border Gateway Protocol (BGP), an IPv6 Intermediate System-to-Intermediate System (IS-IS), or an IPv6 Routing Information Protocol (RIP) routing process can support, use the **maximum-paths** command in address family configuration or router configuration mode. To restore the default value, use the **no** form of this command.

maximum-paths *number-paths*

no maximum-paths

| | | |
|--------------------|---------------------|--|
| Syntax Description | <i>number-paths</i> | Maximum number of equal-cost paths to a destination learned via IPv6 BGP, IS-IS, or RIP installed in the IPv6 routing table, in the range from 1 to 4. The default for BGP is one path; the default for IS-IS and RIP is four paths. |
|--------------------|---------------------|--|

Defaults The default for BGP is one path; the default for IS-IS and RIP is four paths.

Command Modes Address family configuration
Router configuration

| | | |
|-----------------|------------|--|
| Command History | Release | Modification |
| | 12.2(8)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S and support for IPv6 RIP was added. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines The **maximum-paths (IPv6)** command is similar to the **maximum-paths** command, except that it is IPv6-specific.

To configure the **maximum-paths** command for IPv6 BGP and ISIS, enter address family mode.

Examples The following example shows a maximum of three paths to an external destination for the IPv6 BGP autonomous system 65000, and a maximum of two paths to an internal IPv6 BGP destination being configured:

```
Router(config)# router bgp 65000
Router(config-router)# address-family ipv6
Router(config-router-af)# maximum-paths 3
Router(config-router-af)# maximum-paths ibgp 2
```

The following example shows a maximum of two paths to a destination for the IPv6 IS-IS routing process named area01 being configured:

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6
Router(config-router-af)# maximum-paths 2
```

The following example shows a maximum of one path to a destination for the IPv6 RIP routing process named one being configured:

```
Router(config)# ipv6 router rip one
Router(config-rtr-rip)# maximum-paths 1
```

mpls ipv6 source-interface

To specify an IPv6 address of an interface to be used as the source address for locally generated IPv6 packets to be sent over a Multiprotocol Label Switching (MPLS) network, use the **mpls ipv6 source-interface** command in global configuration mode. To disable this feature, use the **no** form of this command.

```
mpls ipv6 source-interface type number

no mpls ipv6 source-interface
```

| | | |
|--------------------|-------------|---|
| Syntax Description | type number | The interface type and number whose IPv6 address is to be used as the source for locally generated IPv6 packets to be sent over an MPLS backbone. |
| | Note | A space between the type and number arguments is not required. |

| | |
|----------|---------------------------|
| Defaults | This feature is disabled. |
|----------|---------------------------|

| | |
|---------------|----------------------|
| Command Modes | Global configuration |
|---------------|----------------------|

| | | |
|-----------------|-----------|---|
| Command History | Release | Modification |
| | 12.0(22)S | This command was introduced. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

| | |
|------------------|---|
| Usage Guidelines | Use this command in conjunction with the neighbor send-label address family configuration command to allow IPv6 traffic to run over an IPv4 MPLS network without any software or hardware configuration changes in the backbone. Edge routers, configured to run both IPv4 and IPv6, forward IPv6 traffic using MPLS and multiprotocol internal BGP (MP-iBGP). |
|------------------|---|

| | |
|----------|--|
| Examples | The following example shows loopback interface 0 being configured as a source address for locally generated IPv6 packets: interface Loopback0 ip address 192.168.99.5 255.255.255.255 ipv6 address 2001:0DB8::1/32 ! mpls ipv6 source-interface loopback0 |
|----------|--|

| | | |
|------------------|---------------------|--|
| Related Commands | Command | Description |
| | neighbor send-label | Advertises the capability of the router to send MPLS labels with BGP routes. |

multi-topology

To enable multitopology Intermediate System-to-Intermediate System (IS-IS) for IPv6, use the **multi-topology** command in address family configuration mode. To disable multitopology IS-IS for IPv6, use the **no** form of this command.

multi-topology [**transition**]

no multi-topology

| | |
|---------------------------|--|
| Syntax Description | transition (Optional) Allows an IS-IS IPv6 user to continue to use single shortest path first (SPF) mode while upgrading to multitopology IS-IS for IPv6. |
|---------------------------|--|

| | |
|-----------------|---|
| Defaults | Multitopology IS-IS is disabled by default. |
|-----------------|---|

| | |
|----------------------|------------------------------|
| Command Modes | Address family configuration |
|----------------------|------------------------------|

| | | |
|-------------------------|----------------|---|
| Command History1 | Release | Modification |
| | 12.2(15)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

| | |
|-------------------------|---|
| Usage Guidelines | By default, the router runs IS-IS IPv6 in single SPF mode. The multi-topology command enables multitopology IS-IS for IPv6. |
| | The optional transition keyword can be used to migrate from IS-IS IPv6 single SPF mode to multitopology IS-IS IPv6. When transition mode is enabled, the router advertises both multitopology type, length, and value (TLV) objects and single-SPF-mode IS-IS IPv6 TLVs, but the SPF is computed using the single-SPF-mode IS-IS IPv6 TLV. This action has the side effect of increasing the link-state packet (LSP) size. |

| | |
|-----------------|---|
| Examples | The following example enables multitopology IS-IS for IPv6: |
|-----------------|---|

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# multi-topology
```

neighbor activate

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

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

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

Syntax Description

| | |
|------------------------|---|
| <i>ip-address</i> | IP address of the neighboring router. |
| <i>peer-group-name</i> | Name of Border Gateway Protocol (BGP) peer group. |
| <i>ipv6-address</i> | IPv6 address of the BGP neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |

Defaults

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



Note

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

Command Modes

Address family configuration
Router configuration

Command History

| Release | Modification |
|------------|---|
| 11.0 | This command was introduced. |
| 12.0(5)T | Support for address family configuration mode and the IPv4 address family were added. |
| 12.2(2)T | The <i>ipv6-address</i> argument and support for the IPv6 address family were added. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

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

Examples

Address Exchange Example for Address Family vpnv4

The following example shows how to enable address exchange for address family vpnv4 for all neighbors in the BGP peer group named PEPEER and for the neighbor 144.0.0.44:

```
Router(config)# address-family vpnv4
Router(config-router-af)# neighbor PEPEER activate
Router(config-router-af)# neighbor 144.0.0.44 activate
Router(config-router-af)# exit-address-family
```

Address Exchange Example for Address Family IPv4 unicast

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

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

Address Exchange Example for Address Family IPv6

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

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

Related Commands

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

neighbor override-capability-neg

To enable the IPv6 address family for a Border Gateway Protocol (BGP) neighbor that does not support capability negotiation, use the **neighbor override-capability-neg** command in address family configuration mode. To disable the IPv6 address family for a BGP neighbor that does not support capability negotiation, use the **no** form of this command.

neighbor {*peer-group-name* | *ipv6-address*} **override-capability-neg**

no neighbor {*peer-group-name* | *ipv6-address*} **override-capability-neg**

Syntax Description

| | |
|------------------------|---|
| <i>peer-group-name</i> | Name of a BGP peer group. |
| <i>ipv6-address</i> | IPv6 address of the BGP neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |

Defaults

Capability negotiation is enabled.

Command Modes

Address family configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

Capability negotiation is used to establish a connection between BGP-speaking peers. If one of the BGP peers does not support capability negotiation, the connection is automatically terminated. The **neighbor override-capability-neg** command overrides the capability negotiation process and enables BGP-speaking peers to establish a connection.

The **neighbor override-capability-neg** command is supported only in address family configuration mode for the IPv6 address family.

Examples

The following example enables the IPv6 address family for BGP neighbor 7000::2:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor 7000::2 override-capability-neg
```

The following example enables the IPv6 address family for all neighbors in the BGP peer group named group1:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group1 override-capability-neg
```

Related Commands

| Command | Description |
|----------------------------|--|
| address-family ipv6 | Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes. |

neighbor send-label

To enable a Border Gateway Protocol (BGP) router to send Multiprotocol Label Switching (MPLS) labels with BGP routes to a neighboring BGP router, use the **neighbor send-label** command in address family configuration mode or router configuration mode. To disable this feature, use the **no** form of this command.

neighbor *ip-address* **send-label**

no neighbor *ip-address* **send-label**

| | | |
|---------------------------|-------------------|---------------------------------------|
| Syntax Description | <i>ip-address</i> | IP address of the neighboring router. |
|---------------------------|-------------------|---------------------------------------|

| | |
|-----------------|---|
| Defaults | By default, BGP routers distribute only BGP routes. |
|-----------------|---|

| | |
|----------------------|--|
| Command Modes | Address family configuration Router configuration |
|----------------------|--|

| Command History | Release | Modification |
|------------------------|------------|---|
| | 12.0(21)ST | This command was introduced. |
| | 12.0(22)S | Support for IPv6 was added. |
| | 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

| | |
|-------------------------|---|
| Usage Guidelines | This command enables a router to use BGP to distribute MPLS labels along with the IPv4 routes to a peer router. You must issue this command on both the local router and the neighboring router. |
| | <p>This command has the following restrictions:</p> <ul style="list-style-type: none"> If a BGP session is running when you issue the neighbor send-label command, the command does not take effect until the BGP session is restarted. In router configuration mode, only IPv4 addresses are distributed. <p>Use this command in IPv6 address family configuration mode to bind and advertise IPv6 prefix MPLS labels. Using this command in conjunction with the mpls ipv6 source-interface global configuration command allows IPv6 traffic to run over an IPv4 MPLS network without any software or hardware configuration changes in the backbone. Edge routers configured to run both IPv4 and IPv6 forward IPv6 traffic using MPLS and multiprotocol internal BGP (MP-iBGP).</p> |

| | |
|-----------------|--|
| Examples | The following example shows how to enable a router in the autonomous system 65000 to send MPLS labels with BGP routes to the neighbor BGP router at 192.168.0.1: |
|-----------------|--|

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.0.1 remote-as 65001
Router(config-router)# neighbor 192.168.0.1 send-label
```

The following example shows how to enable a router in the autonomous system 65000 to bind and advertise IPv6 prefix MPLS labels and send the labels with BGP routes to the neighbor BGP router at 192.168.99.70:

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.99.70 remote-as 65000
Router(config-router)# address-family ipv6
Router(config-router-af)# neighbor 192.168.99.70 activate
Router(config-router-af)# neighbor 192.168.99.70 send-label
```

Related Commands

| Command | Description |
|---------------------------------------|--|
| neighbor activate | Enables the exchange of information with a neighboring router. |
| mpls ipv6 source-interface | Specifies the IPv6 address of an interface to be used as the source address for locally generated IPv6 packets to be sent over a network running MPLS. |

neighbor translate-update

To generate multiprotocol IPv6 Border Gateway Protocol (BGP) updates that correspond to unicast IPv6 updates received from a peer, use the **neighbor translate-update** command in address family or router configuration mode. To return to default values, use the **no** form of the command.

```
neighbor ipv6-address translate-update ipv6 multicast [unicast]

no neighbor ipv6-address translate-update ipv6 multicast [unicast]
```

| | | |
|--------------------|----------------|--|
| Syntax Description | ipv6-address | Resets the TCP connection to the specified IPv6 BGP neighbor and removes all routes learned from the connection from the BGP table. |
| | | This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| | IPv6 multicast | Specifies IPv6 multicast address prefixes. |
| | unicast | (Optional) Specifies IPv6 unicast address prefixes. |

Defaults No BGP updates for unicast IPv6 are updated

Command Modes Address family configuration
Router configuration

| Command History | Release | Modification |
|-----------------|-----------|--|
| | 12.0(26)S | This command was introduced. |
| | 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines The multicast BGP (MBGP) translate-update feature generally is used in an MBGP-capable router that peers with a customer site that has a router that is only BGP capable; the customer site has not or cannot upgrade the router to an MBGP-capable image. Because the customer site cannot originate MBGP advertisements, the router with which it peers will translate the BGP prefixes into MBGP prefixes, which are used for multicast-source Reverse Path Forwarding (RPF) lookup.

Examples The following example generates multiprotocol IPv6 BGP updates that correspond to unicast IPv6 updates received from peer at address 7000::2:

```
neighbor 7000::2 translate-update ipv6 multicast
```

neighbor update-source

To have the Cisco IOS software allow BGP sessions to use any operational interface for TCP connections, use the **neighbor update-source** command in router configuration mode. To restore the interface assignment to the closest interface, which is called the best local address, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type* *interface-number*

no neighbor {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type* *interface-number*

Syntax Description

| | |
|-------------------------|--|
| <i>ip-address</i> | IPv4 address of the BGP-speaking neighbor. |
| <i>ipv6-address</i> | IPv6 address of the BGP-speaking neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| <i>peer-group-name</i> | Name of a BGP peer group. |
| <i>interface-type</i> | Interface type. |
| <i>interface-number</i> | Interface number. |

Defaults

Best local address

Command Modes

Router configuration

Command History

| Release | Modification |
|--|---|
| 10.0 | This command was introduced. |
| 12.2(4)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S | The <i>ipv6-address</i> argument was added. |

Usage Guidelines

This feature can work in conjunction with the loopback interface feature described in the “Interface Configuration Overview” chapter of the Release 12.2, *Cisco IOS Interface Configuration Guide*.

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

The **neighbor update-source** command must be used to enable IPv6 link-local peering for internal or external BGP sessions.

Examples

The following example sources BGP TCP connections for the specified neighbor with the IP address of the loopback interface rather than the best local address:

```
router bgp 110
```

```
network 172.16.0.0
neighbor 172.16.2.3 remote-as 110

neighbor 172.16.2.3 update-source Loopback0
```

The following example sources IPv6 BGP TCP connections for the specified neighbor in autonomous system 110 with the global IPv6 address of loopback interface 0 and the specified neighbor in autonomous system 120 with the link-local IPv6 address of Fast Ethernet interface 0/0:

```
router bgp 110
  neighbor 3FFE::3 remote-as 110
  neighbor 3FFE::3 update-source Loopback0
  neighbor FE80::2 remote-as 120
  neighbor FE80::2 update-source FastEthernet 0/0

address-family ipv6
  neighbor 3FFE::3 activate
  neighbor FE80::2 activate
exit-address-family
```

Related Commands

| Command | Description |
|---------------------------|--|
| neighbor activate | Enables the exchange of information with a BGP neighboring router. |
| neighbor remote-as | Adds an entry to the BGP or multiprotocol BGP neighbor table. |

peer default ipv6 address pool

To specify the pool from which client prefixes are assigned, use the **peer default ipv6 address** command in interface configuration mode. To disable a prior peer IPv6 address pooling configuration on an interface, or to remove the default address from your configuration, use the **no** form of this command.

peer default ipv6 address pool *pool-name*

no peer default ipv6 address pool

| | | |
|---------------------------|--|--|
| Syntax Description | <i>pool-name</i> Name of a local address pool created using the ipv6 local pool command. | |
| Defaults | The default is pool . | |
| Command Modes | Interface configuration | |
| Command History | Release | Modification |
| | 12.2(13)T | This command was introduced. |
| Usage Guidelines | <p>This command applies to point-to-point interfaces that support PPP encapsulation. This command sets the address used on the remote (PC) side.</p> <p>This command allows an administrator to configure all possible address pooling mechanisms on an interface-by-interface basis.</p> | |
| Examples | <p>The following command specifies that this interface will use a local IPv6 address pool named pool3:</p> <pre>peer default ipv6 address pool pool3</pre> <p>In the following example, the "pool1" pool is assigned to Virtual-template1</p> <pre>interface Virtual-Template1 ipv6 enable no ipv6 nd suppress-ra peer default ipv6 address pool pool1 ppp authentication chap</pre> | |
| Related Commands | Command | Description |
| | async dynamic address | Specifies dynamic asynchronous addressing versus default addressing. |
| | encapsulation ppp | Enables PPP encapsulation. |
| | exec | Allows an EXEC process on a line. |

| Command | Description |
|------------------------|---|
| ipv6 local pool | Configures a local pool of IPv6 addresses to be used when a remote peer connects to a point-to-point interface. |
| ppp | Starts an asynchronous connection using PPP. |

permit (IPv6)

To set permit conditions for an IPv6 access list, use the **permit** command in IPv6 access list configuration mode. To remove the permit conditions, use the **no** form of this command.

```
permit {protocol} {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [dscp value] [flow-label value] [fragments] [log] [log-input]
[reflect name [timeout value]] [routing] [sequence value] [time-range name]
```

```
no permit {protocol} {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [dscp value] [flow-label value] [fragments] [log] [log-input]
[reflect name [timeout value]] [routing] [sequence value] [time-range name]
```

Internet Control Message Protocol

```
permit icmp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [icmp-type [icmp-code] | icmp-message] [dscp value] [flow-label
value] [fragments] [log] [log-input] [routing] [sequence value] [time-range name]
```

Transmission Control Protocol

```
permit tcp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [ack] [dscp value] [established] [fin] [flow-label value]
[fragments] [log] [log-input] [neg {port | protocol}] [psh] [range {port | protocol}] [reflect
name [timeout value]] [routing] [rst] [sequence value] [syn] [time-range name] [urg]
```

User Datagram Protocol

```
permit udp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address}
[operator [port-number]] [dscp value] [flow-label value] [fragments] [log] [log-input] [neg
{port | protocol}] [range {port | protocol}] [reflect name [timeout value]] [routing]
[sequence value] [time-range name]
```

Syntax Description

| | |
|---|--|
| <i>protocol</i> | Name or number of an Internet protocol. It can be one of the keywords ahp , esp , icmp , ipv6 , pcp , sctp , tcp , or udp , or an integer in the range from 0 to 255 representing an IPv6 protocol number. |
| <i>source-ipv6-prefix/prefix-length</i> | The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| any | An abbreviation for the IPv6 prefix ::/0. |
| host source-ipv6-address | The source IPv6 host address about which to set permit conditions. This <i>source-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |

| | |
|--|--|
| <i>operator</i> [<i>port-number</i>] | <p>(Optional) Specifies an operand that compares the source or destination ports of the specified protocol. Operands are lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).</p> <p>If the operator is positioned after the <i>source-ipv6-prefix/prefix-length</i> argument, it must match the source port.</p> <p>If the operator is positioned after the <i>destination-ipv6-prefix/prefix-length</i> argument, it must match the destination port.</p> <p>The range operator requires two port numbers. All other operators require one port number.</p> <p>The optional <i>port-number</i> argument is a decimal number or the name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.</p> |
| <i>destination-ipv6-prefix/prefix-length</i> | <p>The destination IPv6 network or class of networks about which to set permit conditions.</p> <p>This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</p> |
| host <i>destination-ipv6-address</i> | <p>The destination IPv6 host address about which to set permit conditions.</p> <p>This <i>destination-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</p> |
| dscp <i>value</i> | <p>(Optional) Matches a differentiated services codepoint value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.</p> |
| flow-label <i>value</i> | <p>(Optional) Matches a flow label value against the flow label value in the Flow Label field of each IPv6 packet header. The acceptable range is from 0 to 1048575.</p> |
| fragments | <p>(Optional) Matches non-initial fragmented packets where the fragment extension header contains a non-zero fragment offset. The fragments keyword is an option only if the <i>operator</i> [<i>port-number</i>] arguments are not specified.</p> |
| log | <p>(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the logging console command.)</p> <p>The message includes the access list name and sequence number, whether the packet was permitted; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted in the prior 5-minute interval.</p> |
| log-input | <p>(Optional) Provides the same function as the log keyword, except that the logging message also includes the input interface.</p> |

| | |
|--|--|
| reflect <i>name</i> | (Optional) Specifies a reflexive IPv6 access list. Reflexive IPv6 access lists are created dynamically when an IPv6 packets matches a permit statement that contains the reflect keyword. The reflexive IPv6 access list mirrors the permit statement and times out automatically when no IPv6 packets match the permit statement. Reflexive IPv6 access lists can be applied to the TCP, UDP, SCTP, and ICMP for IPv6 packets. |
| timeout <i>value</i> | (Optional) Interval of idle time (in seconds) after which a reflexive IPv6 access list times out. The acceptable range is from 1 to 4294967295. The default is 180 seconds. |
| routing | (Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header. |
| sequence <i>value</i> | (Optional) Specifies the sequence number for the access list statement. The acceptable range is from 1 to 4294967295. |
| time-range <i>name</i> | (Optional) Specifies the time range that applies to the permit statement. The name of the time range and its restrictions are specified by the time-range and absolute or periodic commands, respectively. |
| <i>icmp-type</i> | (Optional) Specifies an ICMP message type for filtering ICMP packets. ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255. |
| <i>icmp-code</i> | (Optional) Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255. |
| <i>icmp-message</i> | (Optional) Specifies an ICMP message name for filtering ICMP packets. ICMP packets can be filtered by an ICMP message name or ICMP message type and code. The possible names are listed in the “Usage Guidelines” section. |
| ack | (Optional) For the TCP protocol only: acknowledgment (ACK) bit set. |
| established | (Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection. |
| fin | (Optional) For the TCP protocol only: Fin bit set; no more data from sender. |
| neq { <i>port</i> <i>protocol</i> } | (Optional) Matches only packets that are not on a given port number. |
| psh | (Optional) For the TCP protocol only: Push function bit set. |
| range { <i>port</i> <i>protocol</i> } | (Optional) Matches only packets in the range of port numbers. |
| rst | (Optional) For the TCP protocol only: Reset bit set. |
| syn | (Optional) For the TCP protocol only: Synchronize bit set. |
| urg | (Optional) For the TCP protocol only: Urgent pointer bit set. |

Defaults

No IPv6 access list is defined.

Command Modes

IPv6 access list configuration

Command History

| Release | Modification |
|-----------|---|
| 12.0(23)S | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **permit** (IPv6) command is similar to the **permit** (IP) command, except that it is IPv6-specific.

Use the **permit** (IPv6) command following the **ipv6 access-list** command to define the conditions under which a packet passes the access list or to define the access list as a reflexive access list.

Specifying IPv6 for the *protocol* argument matches against the IPv6 header of the packet.

By default, the first statement in an access list is number 10, and the subsequent statements are incremented by 10.

You can add **permit**, **deny**, **remark**, or **evaluate** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

In Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, and 12.0(22)S, IPv6 access control lists (ACLs) are defined and their deny and permit conditions are set by using the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode. In Cisco IOS Release 12.0(23)S or later releases, IPv6 ACLs are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Refer to the **ipv6 access-list** command for more information on defining IPv6 ACLs.



Note

In Cisco IOS Release 12.0(23)S or later releases, every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect.

The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Both the *source-ipv6-prefix/prefix-length* and *destination-ipv6-prefix/prefix-length* arguments are used for traffic filtering (the source prefix filters traffic based upon the traffic source; the destination prefix filters traffic based upon the traffic destination).



Note

IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified.

The following is a list of ICMP message names:

- beyond-scope
- destination-unreachable

- echo-reply
- echo-request
- header
- hop-limit
- mld-query
- mld-reduction
- mld-report
- nd-na
- nd-ns
- next-header
- no-admin
- no-route
- packet-too-big
- parameter-option
- parameter-problem
- port-unreachable
- reassembly-timeout
- renum-command
- renum-result
- renum-seq-number
- router-advertisement
- router-renumbering
- router-solicitation
- time-exceeded
- unreachable

Defining Reflexive Access Lists

To define an IPv6 reflexive list, a form of session filtering, use the **reflect** keyword in the **permit** (IPv6) command. The **reflect** keyword creates an IPv6 reflexive access list and triggers the creation of entries in the reflexive access list. The **reflect** keyword must be an entry (condition statement) in an IPv6 access list.



Note

For IPv6 reflexive access lists to work, you must nest the reflexive access list using the **evaluate** command.

If you are configuring IPv6 reflexive access lists for an external interface, the IPv6 access list should be one that is applied to outbound traffic.

If you are configuring an IPv6 reflexive access list for an internal interface, the IPv6 access list should be one that is applied to inbound traffic.

IPv6 sessions that originate from within your network are initiated with a packet exiting your network. When such a packet is evaluated against the statements in the IPv6 access list, the packet is also evaluated against the IPv6 reflexive permit entry.

As with all IPv6 access list entries, the order of entries is important, because they are evaluated in sequential order. When an IPv6 packet reaches the interface, it will be evaluated sequentially by each entry in the access list until a match occurs.

If the packet matches an entry prior to the reflexive permit entry, the packet will not be evaluated by the reflexive permit entry, and no temporary entry will be created for the reflexive access list (session filtering will not be triggered).

The packet will be evaluated by the reflexive permit entry if no other match occurs first. Then, if the packet matches the protocol specified in the reflexive permit entry, the packet is forwarded and a corresponding temporary entry is created in the reflexive access list (unless the corresponding entry already exists, indicating that the packet belongs to a session in progress). The temporary entry specifies criteria that permit traffic into your network only for the same session.

Characteristics of Reflexive Access List Entries

The **permit** (IPv6) command with the **reflect** keyword enables the creation of temporary entries in the same IPv6 reflexive access list that was defined by the **permit** (IPv6) command. The temporary entries are created when an IPv6 packet exiting your network matches the protocol specified in the **permit** (IPv6) command. (The packet “triggers” the creation of a temporary entry.) These entries have the following characteristics:

- The entry is a permit entry.
- The entry specifies the same IP upper-layer protocol as the original triggering packet.
- The entry specifies the same source and destination addresses as the original triggering packet, except that the addresses are swapped.
- If the original triggering packet is TCP or UDP, the entry specifies the same source and destination port numbers as the original packet, except that the port numbers are swapped.
- If the original triggering packet is a protocol other than TCP or UDP, port numbers do not apply, and other criteria are specified. For example, for ICMP, type numbers are used: The temporary entry specifies the same type number as the original packet (with only one exception: if the original ICMP packet is type 8, the returning ICMP packet must be type 0 to be matched).
- The entry inherits all the values of the original triggering packet, with exceptions only as noted in the previous four bullets.
- IPv6 traffic entering your internal network will be evaluated against the entry, until the entry expires. If an IPv6 packet matches the entry, the packet will be forwarded into your network.
- The entry will expire (be removed) after the last packet of the session is matched.
- If no packets belonging to the session are detected for a configured length of time (the timeout period), the entry will expire.

Examples

The following example configures two IPv6 access lists named OUTBOUND and INBOUND and applies both access lists to outbound and inbound traffic on Ethernet interface 0. The first and second permit entries in the OUTBOUND list permit all TCP and UDP packets from network 2001:0DB8:0300:0201::/64 to exit out of Ethernet interface 0. The entries also configure the temporary IPv6 reflexive access list named REFLECTOUT to filter returning (incoming) TCP and UDP packets on Ethernet interface 0. The first deny entry in the OUTBOUND list keeps all packets from the network

FEC0:0:0:0201::/64 (packets that have the site-local prefix FEC0:0:0:0201 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0. The third permit entry in the OUTBOUND list permits all ICMP packets to exit out of Ethernet interface 0.

The permit entry in the INBOUND list permits all ICMP packets to enter Ethernet interface 0. The **evaluate** command in the list applies the temporary IPv6 reflexive access list named REFLECTOUT to inbound TCP and UDP packets on Ethernet interface 0. When outgoing TCP or UDP packets are permitted on Ethernet interface 0 by the OUTBOUND list, the INBOUND list uses the REFLECTOUT list to match (evaluate) the returning (incoming) TCP and UDP packets. Refer to the **evaluate** command for more information on nesting IPv6 reflexive access lists within IPv6 ACLs.

```
ipv6 access-list OUTBOUND
 permit tcp 2001:0DB8:0300:0201::/64 any reflect REFLECTOUT
 permit udp 2001:0DB8:0300:0201::/64 any reflect REFLECTOUT
 deny FEC0:0:0:0201::/64 any
 permit icmp any any

ipv6 access-list INBOUND
 permit icmp any any
 evaluate REFLECTOUT

interface ethernet 0
 ipv6 traffic-filter OUTBOUND out
 ipv6 traffic-filter INBOUND in
```



Note

Given that a **permit any any** statement is not included as the last entry in the OUTBOUND or INBOUND access list, only TCP, UDP, and ICMP packets will be permitted out of and in to Ethernet interface 0 (the implicit deny all condition at the end of the access list denies all other packet types on the interface).

Related Commands

| Command | Description |
|------------------------------|---|
| ipv6 access-list | Defines an IPv6 access list and enters IPv6 access list configuration mode. |
| ipv6 traffic-filter | Filters incoming or outgoing IPv6 traffic on an interface. |
| deny (IPv6) | Sets deny conditions for an IPv6 access list. |
| evaluate (IPv6) | Nests an IPv6 reflexive access list within an IPv6 access list. |
| show ipv6 access-list | Displays the contents of all current IPv6 access lists. |

ping

To diagnose basic network connectivity on Apollo, AppleTalk, Connectionless Network Service (CLNS), DECnet, IP, IPv6, Novell IPX, VINES, or XNS networks, use the **ping** (packet internet groper) command in user EXEC or privileged EXEC mode.

ping [*protocol* | **tag**] {*host-name* | *system-address*} [**data** [*hex-data-pattern*]] | **df-bit** | **repeat** [*repeat-count*] | **size** [*datagram-size*] | **source** [*source-address* | **async** | **bvi** | **ctunnel** | **dialer** | **ethernet** | **fastEthernet** | **lex** | **loopback** | **multilink** | **null** | **port-channel** | **tunnel** | **vif** | **virtual-template** | **virtual-tokenring** | **xtagatm**] | **timeout** [*seconds*] | **validate**

Syntax Description

| | |
|--------------------------|---|
| <i>protocol</i> | (Optional) Protocol keyword, one of apollo , appletalk , clns , decnet , ip , ipx , srb , vines , or xns . |
| tag | (Optional) Specifies a tag encapsulated IP ping. |
| <i>host-name</i> | Host name of the system to ping. |
| <i>system-address</i> | Address of the system to ping. |
| data | (Optional) Specifies the data pattern. |
| <i>hex-data-pattern</i> | (Optional) Range is from 0 to FFFF. |
| df-bit | (Optional) Enables the “do-not-fragment” bit in the IP header. |
| repeat | (Optional) Specifies the number of pings sent. The default is 5. |
| <i>repeat-count</i> | (Optional) Range is from 1 to 2147483647. |
| size | (Optional) Specifies the datagram size. Datagram size is the number of bytes in each ping. |
| <i>datagram-size</i> | (Optional) Range is from 40 to 18024. |
| source | (Optional) Specifies the source address or name. |
| <i>source-address</i> | (Optional) Source address or name. |
| async | (Optional) Asynchronous interface. |
| bvi | (Optional) Bridge-Group Virtual Interface. |
| ctunnel | (Optional) CTunnel interface. |
| dialer | (Optional) Dialer interface. |
| ethernet | (Optional) Ethernet IEEE 802.3. |
| fastEthernet | (Optional) FastEthernet IEEE 802.3. |
| lex | (Optional) Lex interface. |
| loopback | (Optional) Loopback interface. |
| multilink | (Optional) Multilink-group interface. |
| null | (Optional) Null interface. |
| port-channel | (Optional) Ethernet channel of interfaces. |
| tunnel | (Optional) Tunnel interface. |
| vif | (Optional) PGM Multicast Host interface. |
| virtual-template | (Optional) Virtual Template interface. |
| virtual-tokenring | (Optional) Virtual Token Ring. |
| xtagatm | (Optional) Extended Tag ATM interface. |
| timeout | (Optional) Specifies the timeout interval in seconds. The default is 2 seconds. |

| | |
|-----------------|--------------------------------------|
| seconds | (Optional) Range is from 0 to 3600. |
| validate | (Optional) Validates the reply data. |

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|------------|---|
| 10.0 | This command was introduced. |
| 12.2(2)T | Support for IPv6 was added. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(11)T | The ping command test characters for IPv6 have been updated. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The user-level ping feature provides a basic ping facility for users that do not have system privileges. This feature allows the Cisco IOS software to perform the simple default ping functionality for a number of protocols. Only the terse form of the **ping** command is supported for user-level pings.

The ping program sends an echo request packet to an address, then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

If the system cannot map an address for a host name, it returns an “%Unrecognized host or address, or protocol not running” message.

To abnormally terminate a ping session, type the escape sequence—by default, Ctrl-^ X. You type the default by simultaneously pressing and releasing the Ctrl, Shift, and 6 keys, and then pressing the X key.

Table 18 describes the characters displayed by the ping facility in IPv4.

Table 18 *ping Test Characters (IPv4)*

| Character | Description |
|-----------|--|
| ! | Each exclamation point indicates receipt of a reply. |
| . | Each period indicates that the network server timed out while waiting for a reply. |
| U | A destination unreachable error protocol data unit (PDU) was received. |
| C | A congestion experienced packet was received. |
| I | User interrupted test. |
| ? | Unknown packet type. |
| & | Packet lifetime exceeded |

Table 19 describes the characters displayed by the ping facility in IPv6.

Table 19 *ping Test Characters (IPv6)*

| | |
|---|---|
| ! | Each exclamation point indicates receipt of a reply. |
| . | Each period indicates that the network server timed out while waiting for a reply. |
| ? | Unknown error. |
| @ | Unreachable for unknown reason. |
| A | Administratively unreachable. Usually, this output indicates that an access list is blocking traffic. |
| B | Packet too big. |
| H | Host unreachable. |
| N | Network unreachable (beyond scope). |
| P | Port unreachable. |
| R | Parameter problem. |
| T | Time exceeded. |
| U | No route to host. |

**Note**

Not all protocols require hosts to support pings. For some protocols, the pings are Cisco-defined and are only answered by another Cisco router.

Examples

The following user EXEC example shows sample ping output for the IPv6 host named *host1*:

```
Router> ping host1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to FE80::260:3EFF:FE11:6770, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent, round-trip min/avg/max = 1/3/4 ms
```

After you enter the **ping** command in privileged mode, the system prompts for one of the following protocol keywords: **apollo**, **appletalk**, **clns**, **decnet**, **ip**, **ipv6**, **ipx**, **vines**, or **xns**. The default protocol is IP.

If you enter a host name or address on the same line as the **ping** command, the default action is taken as appropriate for the protocol type of that name or address.

Although the precise dialog varies somewhat from protocol to protocol, all are similar to the ping session using default values shown in the following output:

```
Router# ping
```

```
Protocol [ip]: ipv6
```

```
Target IPv6 address: FE80::260:3EFF:FE11:6770
```

```
Repeat count [5]:
```

```
Datagram size [100]:
```

```
Timeout in seconds [2]:
```

```
Extended commands? [no]:
```

```
Output Interface:
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to FE80::260:3EFF:FE11:6770, timeout is 2 seconds:
```

```
!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms



Note

In Cisco IOS Release 12.2(8)T or later releases, an IPv6 address enclosed in square brackets ([]), such as [FE80::260:3EFF:FE11:6770] in the example, is acceptable to the system. Refer to RFC 2732, *Format for Literal IPv6 Addresses in URL's*, for more information on the use of square brackets with literal IPv6 addresses in URLs.

Table 20 describes the default **ping** fields shown in the display.

Table 20 *ping Field Descriptions*

| Field | Description |
|--|--|
| Protocol [ip]: | Prompts for a supported protocol. Enter apollo , appletalk , clns , decnet , ip , ipv6 , ipx , vines , or xns . Default: IP. |
| Target IP address: | Prompts for the address or host name of the destination node you plan to ping. If you have specified a supported protocol other than IP (the default protocol), enter an appropriate address for that protocol here. Default: none. |
| Repeat count [5]: | Number of ping packets that will be sent to the destination address. Default: 5. |
| Datagram size [100]: | Size of the ping packet (in bytes). Default: 100 bytes. |
| Timeout in seconds [2]: | Timeout interval (in seconds). Default: 2. |
| Extended commands [n]: | Specifies whether a series of additional commands appears. Default: no. In an IPv6 dialog for the ping command, entering yes in the Extended commands [n] field displays the UDP protocol? [no], Priority [0], and Include extension headers? [no] fields. |
| UDP protocol? [no]: (not shown in sample output) | Specifies UDP packets or ICMPv6 packets. Default: no (ICMP packets are sent). |
| Priority [0]: (not shown in sample output) | Specifies the traffic class. Default is 0. |
| Include extension headers? [no]: (not shown in sample output) | Includes destination options extension headers in the echo request packets. Default: no. |
| Output Interface: | Specifies the interface out of which the echo request packet is sent to the destination node. Default: determined by the router. |
| Sweep range of sizes [n]: (not shown in sample output) | Allows you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the maximum transmission units (MTUs) configured on the nodes along the path to the destination address. Packet fragmentation contributing to performance problems can then be reduced. (This field is not included in the IPv6 dialog for the ping command.) |
| !!!! | Each exclamation point (!) indicates receipt of a reply. A period (.) indicates that the network server timed out while waiting for a reply. Other characters may appear in the ping output display, depending on the protocol type. |

Table 20 *ping Field Descriptions (continued)*

| Field | Description |
|-----------------------------------|--|
| Success rate is 100 percent | Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic. |
| round-trip min/avg/max = 1/2/4 ms | Round-trip minimum, average, and maximum time intervals for the protocol echo packets (in milliseconds). |

ping ipv6

To diagnose basic network connectivity when using IPv6, use the **ping IPv6** command in user EXEC or privileged EXEC mode.

ping ipv6 *ipv6-address* [**data** *hex-data-pattern* | **repeat** *repeat-count* | **size** *datagram-size* | **source** [**async** | **bvi** | **ctunnel** | **dialer** | **ethernet** | **fastEthernet** | **gigabitEthernet** | **loopback** | **mfr** | **multilink** | **null** | **port-channel** | **tunnel** | **virtual-template** | *source-address* | **xtagatm**] | **timeout** *seconds* | **verbose**]

Syntax Description

| | |
|-------------------------|--|
| <i>ipv6-address</i> | The address or hostname of the IPv6 host to be pinged. This address or hostname must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons. |
| data | (Optional) Specifies the data pattern. |
| <i>hex-data-pattern</i> | (Optional) Range is from 0 to FFFF. |
| repeat | (Optional) Specifies the number of pings sent. The default is 5. |
| <i>repeat-count</i> | (Optional) Range is from 1 to 2147483647. |
| size | (Optional) Specifies the datagram size. Datagram size is the number of bytes in each ping. |
| <i>datagram-size</i> | (Optional) Range is from 48 to 18024. |
| source | (Optional) Specifies the source address or name. |
| async | (Optional) Asynchronous interface. |
| bvi | (Optional) Bridge-Group Virtual Interface. |
| ctunnel | (Optional) CTunnel interface. |
| dialer | (Optional) Dialer interface. |
| ethernet | (Optional) Ethernet IEEE 802.3. |
| fastEthernet | (Optional) FastEthernet IEEE 802.3. |
| gigabitEthernet | (Optional) GigabitEthernet IEEE 802.3z. |
| loopback | (Optional) Loopback interface. |
| mfr | (Optional) Multilink frame relay (MFR) bundle interface. |
| multilink | (Optional) Multilink-group interface. |
| null | (Optional) Null interface. |
| port-channel | (Optional) Ethernet channel of interfaces. |
| tunnel | (Optional) Tunnel interface. |
| virtual-template | (Optional) Virtual Template interface. |
| <i>source-address</i> | (Optional) Source IPv6 address or name. |
| xtagatm | (Optional) Extended Tag ATM interface. |
| timeout | (Optional) Specifies the timeout interval in seconds. The default is 2 seconds. |
| <i>seconds</i> | (Optional) Range is from 0 to 3600. |
| verbose | (Optional) Displays the verbose output. |

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|----------|------------------------------|
| 12.3(4)T | This command was introduced. |

Usage Guidelines

The user-level ping feature provides a basic ping facility for users that do not have system privileges. This feature allows the Cisco IOS software to perform the simple default ping functionality for a number of protocols.

The ping program sends an echo request packet to an address, then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

If the system cannot map an address for a host name, it returns an “%Unrecognized host or address, or protocol not running” message.

To abnormally terminate a ping session, type the escape sequence—by default, Ctrl-^ X. You type the default by simultaneously pressing and releasing the Ctrl, Shift, and 6 keys, and then pressing the X key.

**Caution**

When the **timeout** keyword is used with the *seconds* argument set to 0, an immediate timeout occurs, which causes a flood ping. Use the **timeout 0** parameter with caution, because you may only receive replies from immediately adjacent routers depending on router and network utilization, distance to the remote device, and other factors.

Table 19 describes the characters displayed by the ping facility in IPv6.

Table 21 *ping Test Characters (IPv6)*

| | |
|---|---|
| ! | Each exclamation point indicates receipt of a reply. |
| . | Each period indicates that the network server timed out while waiting for a reply. |
| ? | Unknown error. |
| @ | Unreachable for unknown reason. |
| A | Administratively unreachable. Usually, this output indicates that an access list is blocking traffic. |
| B | Packet too big. |
| H | Host unreachable. |
| N | Network unreachable (beyond scope). |
| P | Port unreachable. |
| R | Parameter problem. |
| T | Time exceeded. |
| U | No route to host. |

**Note**

Not all protocols require hosts to support pings. For some protocols, the pings are Cisco-defined and are only answered by another Cisco router.

When the **ping ipv6** command is enabled, the router attempts to resolve host names into IPv6 addresses before trying to resolve them into IPv4 addresses, so if a host name resolves to both an IPv6 and an IPv4 address and you specifically want to use the IPv4 address, use the **ping** (IPv4) command.

Examples

The following user EXEC example shows sample output for the **ping ipv6** command:

```
Router# ping ipv6

Target IPv6 address: 2001:0DB8::3/64
Repeat count [5]:
Datagram size [100]:48
Timeout in seconds [2]:
Extended commands? [no]: yes
UDP protocol? [no]:
Verbose? [no]:
Precedence [0]:
DSCP [0]:
Include hop by hop option? [no]:yes
Include destination option? [no]:y
% Using size of 64 to accomodate extension headers
Sweep range of sizes? [no]:y
Sweep min size [100]: 100
Sweep max size [18024]: 150
Sweep interval [1]: 5
Sending 55, [100..150]-byte ICMP Echos to 2001:0DB8::3/64, timeout is 2 seconds:
Success rate is 100 percent
round-trip min/avg/max = 2/5/10 ms
```

Table 20 describes the default **ping IPv6** fields shown in the display.

Table 22 *ping Field Descriptions*

| Field | Description |
|-------------------------|--|
| Target IPv6 address: | Prompts for the IPv6 address or host name of the destination node you plan to ping. Default: none. |
| Repeat count [5]: | Number of ping packets that will be sent to the destination address. Default: 5. |
| Datagram size [100]: | Size of the ping packet (in bytes). Default: 100 bytes. |
| Timeout in seconds [2]: | Timeout interval (in seconds). Default: 2. |
| Extended commands [no]: | Specifies whether a series of additional commands appears. Default: no. In an IPv6 dialog for the ping IPv6 command, entering yes in the Extended commands field displays the UDP protocol?, Verbose, Priority, and Include extension headers? fields. |
| UDP protocol? [no]: | Specifies UDP packets or ICMPv6 packets. Default: no (ICMP packets are sent). |
| Verbose? [no]: | Enables verbose output. |

Table 22 ping Field Descriptions (continued)

| Field | Description |
|---|---|
| Precedence [0]: | Sets precedence in the IPv6 header. The range is from 0 to 7. |
| DSCP [0]: | Sets DSCP in the IPv6 header. The range is from 0 to 63. DSCP only appears if the precedence option is not set, because precedence and DSCP are two separate ways of viewing the same bits in the header. |
| Include hop by hop option? [no]: | The IPv6 hop-by-hop option is included in the outgoing echo request header, requiring the ping packet to be examined by each node along the path and therefore not be fast-switched or CEF-switched. This function may help with debugging network connectivity, especially switching problems. Note A Cisco router also includes the hop-by-hop option in the returned echo reply, so the packets should be process-switched rather than fast-switched or CEF-switched on the return path also. Non-Cisco routers likely do not have this option in their echo reply; therefore, if the echo request with hop-by-hop option arrives at the destination but the echo reply does not come back and the destination is not a Cisco router, a fast-path issue may exist in an intermediate router. |
| Include destination option? [no]: | Includes an IPv6 destination option in the outgoing echo request header. |
| Sweep range of sizes? [no]: | Allows you to vary the sizes of the echo packets being sent. This capability is useful for determining the minimum sizes of the maximum transmission units (MTUs) configured on the nodes along the path to the destination address. Packet fragmentation contributing to performance problems can then be reduced. |
| Sweep min size [100]: Sweep max size [18024]: Sweep interval [1]: | Options that appear if “Sweep range of sizes?” option is enabled. <ul style="list-style-type: none"> • Sweep min size—Defaults to the configured “Datagram size” parameter and will override that value if specified. • Interval—The size of the intervals between the “Sweep min size” and “Sweep max size” parameters. For example, min of 100 max of 150 with an interval of 5 means packets sent are of 100, 105, 110, ..., 150 bytes in size. |
| Sending 100, [100..150]-byte ICMP Echos to ... | Minimum and maximum sizes and interval as configured in “Sweep range of sizes” options. Sizes are reported if the ping fails (but not if it succeeds, unless the verbose option is enabled). |
| Success rate is 100 percent | Percentage of packets successfully echoed back to the router. Anything less than 80 percent is usually considered problematic. |
| round-trip min/avg/max = x/x/x ms | Round-trip minimum, average, and maximum time intervals for the protocol echo packets (in milliseconds). |

poison-reverse (IPv6 RIP)

To configure the poison reverse processing of IPv6 Routing Information Protocol (RIP) router updates, use the **poison-reverse** command in router configuration mode. To disable the poison reverse processing of IPv6 RIP updates, use the **no** form of this command.

poison-reverse

no poison-reverse

Syntax Description This command has no keywords or arguments

Defaults Poison reverse is not configured.

Command Modes Router configuration

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines This command configures poison reverse processing of IPv6 RIP router updates. When poison reverse is configured, routes learned via 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.

Examples The following example configures poison reverse processing for the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-rtr-rip)# poison-reverse
```

| Related Commands | Command | Description |
|------------------|---------------------------------|--|
| | split-horizon (IPv6 RIP) | Configure split horizon processing of IPv6 RIP router updates. |

port (IPv6 RIP)

To configure a specified User Datagram Protocol (UDP) port and multicast address for an IPv6 Routing Information Protocol (RIP) routing process, use the **port** command in router configuration mode. To return the port number and multicast address to their default values, use the **no** form of this command.

port *port-number* **multicast-group** *multicast-address*

no *port* *port-number* **multicast-group** *multicast-address*

Syntax Description

| | |
|--------------------------|--|
| <i>port-number</i> | The UDP port number. Can be a number from 1 to 65535. Table 23 in the “Usage Guidelines” section lists common UDP services and their port numbers. |
| multicast-group | Specifies a multicast group. |
| <i>multicast-address</i> | The address or host name of the multicast group. |

Defaults

UDP port 521; multicast address FF02::9

Command Modes

Router configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

Two IPv6 RIP routing processes cannot use the same UDP port. If two IPv6 RIP routing processes are configured on the same UDP port, the second process will not start up until the configuration conflict is resolved. Two IPv6 RIP routing processes can use the same multicast address.

Table 23 Common UDP Services and Their Port Numbers

| Service | Port |
|---|------|
| Domain Name System (DNS) | 53 |
| Network File System (NFS) | 2049 |
| remote-procedure call (RPC) | 111 |
| Simple Network Management Protocol (SNMP) | 161 |
| Trivial File Transfer Protocol (TFTP) | 69 |

Examples

The following example configures UDP 200 and multicast address FF02::9 for the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco  
Router(config-rtr-rip)# port 200 multicast-group FF02::9
```

prc-interval (IPv6)

To configure the hold-down period between partial route calculations (PRCs), use the **prc-interval** command in address family configuration mode. To restore the default interval, use the **no** form of this command.

prc-interval *seconds* [*initial-wait*] [*secondary-wait*]

no prc-interval *seconds*

| | | |
|--------------------|-----------------------|--|
| Syntax Description | <i>seconds</i> | Minimum amount of time between PRCs, in seconds. It can be a number in the range 1 to 120. The default is 5 seconds. |
| | <i>initial-wait</i> | (Optional) Length of time before the first PRC in milliseconds. |
| | <i>secondary-wait</i> | (Optional) Minimum length of time between the first and second PRC in milliseconds |

| | |
|----------|-----------|
| Defaults | 5 seconds |
|----------|-----------|

| | |
|---------------|------------------------------|
| Command Modes | Address family configuration |
|---------------|------------------------------|

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.2(15)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

| | |
|------------------|---|
| Usage Guidelines | The prc-interval command is used only in multitopology IS-IS. |
| | The prc-interval command controls how often Cisco IOS software can perform a PRC. Increasing the PRC interval reduces the processor load of the router, but it could slow the convergence. |
| | This command is analogous to the spf-interval command, which controls the hold-down period between shortest path first (SPF) calculations. |
| | You can use the prc-interval (IPv6) command only when using the Intermediate System-to-Intermediate System (IS-IS) multitopology for IPv6 feature. |

| | |
|----------|--|
| Examples | The following example sets the PRC calculation interval to 20 seconds: |
| | Router(config)# router isis |
| | Router(config-router)# address-family ipv6 |
| | Router(config-router-af)# prc-interval 20 |

Related Commands

| Command | Description |
|----------------------------|---|
| spf-interval (IPv6) | Controls how often Cisco IOS software performs the SPF calculation. |

prefix-delegation

To specify a manually configured numeric prefix to be delegated to a specified client (and optionally a specified identity association for prefix delegation [IAPD] for that client), use the **prefix-delegation** command in DHCP for IPv6 pool configuration mode. To remove the prefix, use the **no** form of this command.

prefix-delegation *ipv6-prefix/prefix-length client-DUID* [**iaid** *iaid*] [**lifetime**]

no prefix-delegation *ipv6-prefix/prefix-length client-DUID* [**iaid** *iaid*]

| | | |
|--------------------|-------------------------|---|
| Syntax Description | <i>ipv6-prefix</i> | (Optional) Specified IPv6 prefix. 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>lprefix-length</i> | The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). |
| | <i>client-DUID</i> | The DHCP unique identifier (DUID) of the client to which the prefix is delegated. |
| | iaid <i>iaid</i> | Identity association identifier (IAID), which uniquely identifies an IAPD on the client. |
| | lifetime | (Optional) Sets a length of time over which the requesting router is allowed to use the prefix. The following values can be used: valid-lifetime —The length of time, in seconds, that the prefix remains valid for the requesting router to use. at —Specifies absolute points in time where the prefix is no longer valid and no longer preferred. infinite —Indicates an unlimited lifetime. preferred-lifetime —The length of time, in seconds, that the prefix remains preferred for the requesting router to use. valid-month valid-date valid-year valid-time —A fixed duration of time for hosts to remember router advertisements. The format to be used can be oct 24 2003 11:45 or 24 oct 2003 11:45 . preferred-month preferred-date preferred-year preferred-time —A fixed duration of time for hosts to remember router advertisements. The format to be used can be oct 24 2003 11:45 or 24 oct 2003 11:45 . |

Defaults No manually configured prefix delegations exist.

Command Modes DHCP for IPv6 pool configuration

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.3(4)T | This command was introduced. |

Usage Guidelines

Administrators can manually configure a list of prefixes and associated preferred and valid lifetimes for an IAPD of a specific client that is identified by its DUID. This static binding of client and prefixes can be specified based on users' subscription to an ISP using the **prefix-delegation** *prefix-length* command.

The *client-DUID* argument identifies the client to which the prefix is delegated. All the configured prefixes will be assigned to the specified IAPD of the client. The IAPD to which the prefix is assigned is identified by the **iaid** argument if the **iaid** keyword is configured. If the **iaid** keyword is not configured, the prefix will be assigned to the first IAPD from the client that does not have a static binding. This function is intended to make it convenient for administrators to manually configure prefixes for a client that only sends one IAPD in case it is not easy to know the **iaid** in advance.

When the delegating router receives a request from a client, it checks whether there is a static binding configured for the IAPD in the client's message. If one is present, the prefixes in the binding are returned to the client. If no such binding is found, the server attempts to assign prefixes for the client from other sources.

Optionally valid and preferred lifetimes can be specified for the prefixes assigned from this pool. Users should coordinate the specified lifetimes with the lifetimes on prefixes from the upstream delegating router if the prefixes were acquired from that router.

The **lifetime** keyword can be specified in one of two ways:

- A fixed duration that stays the same in consecutive advertisements.
- Absolute expiration time in the future so that advertised lifetime decrements in real time, which will result in a lifetime of 0 at the specified time in the future.

The specified length of time is between 60 and 4294967295 seconds or infinity if the **infinite** keyword is specified.

Examples

The following example configures an IAPD for a specified client:

```
prefix-delegation 2001:0DB8::/64 00030001000BBFAA2408
```

Related Commands

| Command | Description |
|-------------------------------|--|
| ipv6 dhcp pool | Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode. |
| ipv6 local pool | Configures a local IPv6 prefix pool. |
| prefix-delegation pool | Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients. |
| show ipv6 dhcp pool | Displays DHCP for IPv6 configuration pool information. |

prefix-delegation pool

To specify a named IPv6 local prefix pool from which prefixes are delegated to Dynamic Host Configuration Protocol (DHCP) for IPv6 clients, use the **prefix-delegation pool** command in DHCP for IPv6 pool configuration mode. To remove a named IPv6 local prefix pool, use the **no** form of this command.

prefix-delegation pool *poolname* [**lifetime**]

no prefix-delegation pool *poolname*

Syntax Description

| | |
|-----------------|--|
| <i>poolname</i> | User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0). |
| lifetime | <p>(Optional) Used to set a length of time for the hosts to remember router advertisements. The following values can be used:</p> <p>valid-lifetime—The length of time, in seconds, that the prefix remains valid for the requesting router to use.</p> <p>at—Specifies absolute points in time where the prefix is no longer valid and no longer preferred.</p> <p>infinite—Indicates an unlimited lifetime.</p> <p>preferred-lifetime—The length of time, in seconds, that the prefix remains preferred for the requesting router to use.</p> <p>valid-month valid-date valid-year valid-time—A fixed duration of time for hosts to remember router advertisements. The format to be used can be oct 24 2003 11:45 or 24 oct 2003 11:45.</p> <p>preferred-month preferred-date preferred-year preferred-time—A fixed duration of time for hosts to remember router advertisements. The format to be used can be oct 24 2003 11:45 or 24 oct 2003 11:45.</p> <p>If the optional lifetime keyword is configured, both valid and preferred lifetimes must be configured.</p> |

Defaults

No IPv6 local prefix pool is specified.
Valid lifetime is 2592000 seconds (30 days).
Preferred lifetime is 604800 seconds (7 days)

Command Modes

DHCP for IPv6 pool configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.3(4)T | This command was introduced. |

Usage Guidelines

The **prefix-delegation pool** command specifies a named IPv6 local prefix pool from which prefixes are delegated to clients. Use the **ipv6 local pool** command to configure the named IPv6 prefix pool.

Optionally, valid and preferred lifetimes can be specified for the prefixes assigned from this pool. Users should coordinate the specified lifetimes with the lifetimes on prefixes from the upstream delegating router if the prefixes were acquired from that router.

The **lifetime** keyword can be specified in one of two ways:

- A fixed duration that stays the same in consecutive advertisements.
- Absolute expiration time in the future so that advertised lifetime decrements in real time, which will result in a lifetime of 0 at the specified time in the future.

The specified length of time is from 60 to 4,294,967,295 seconds or infinity if the **infinite** keyword is specified.

The Cisco IOS DHCP for IPv6 server can assign prefixes dynamically from an IPv6 local prefix pool, which is configured using the **ipv6 local pool** command and associated with a DHCP for IPv6 configuration pool using the **prefix-delegation pool** command. When the server receives a prefix request from a client, it attempts to obtain unassigned prefixes, if any, from the pool.

After the client releases the previously assigned prefixes, the server will return the prefixes to the pool for reassignment to other clients.

Examples

The following example specifies that prefix requests should be satisfied from the pool called client-prefix-pool. The prefixes should be delegated with the valid lifetime set to 1800 seconds, and the preferred lifetime is set to 600 seconds:

```
prefix-delegation pool client-prefix-pool lifetime 1800 600
```

Related Commands

| Command | Description |
|----------------------------|---|
| ipv6 dhcp pool | Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode. |
| ipv6 local pool | Configures a local IPv6 prefix pool. |
| prefix-delegation | Specifies a manually configured numeric prefix that is to be delegated to a particular client's IAPD. |
| show ipv6 dhcp pool | Displays DHCP for IPv6 configuration pool information. |

protocol ipv6 (ATM)

To map the IPv6 address of a remote node to the ATM permanent virtual circuit (PVC) used to reach the address, use the **protocol ipv6** command in ATM VC configuration mode. To remove the static map, use the **no** form of this command.

```
protocol ipv6 ipv6-address [[no] broadcast]

no protocol ipv6 ipv6-address [[no] broadcast]
```

| | | |
|--------------------|--------------|---|
| Syntax Description | ipv6-address | Destination IPv6 (protocol) address that is being mapped to a PVC. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| | no broadcast | (Optional) Indicates whether the map entry should be used when IPv6 multicast packets (not broadcast packets) are sent to the interface. Pseudobroadcasting is supported. The [no] broadcast keywords in the protocol ipv6 command take precedence over the broadcast command configured on the same ATM PVC. |

Defaults No mapping is defined.

Command Modes ATM VC configuration (for an ATM PVC)

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Examples In the following example, two nodes named Cisco 1 and Cisco 2 are connected by a single PVC. The point-to-point subinterface ATM0.132 is used on both nodes to terminate the PVC; therefore, the mapping between the IPv6 addresses of both nodes and the PVC is implicit (no additional mappings are required).

```
Cisco 1 Configuration

interface ATM0
 no ip address
!
interface ATM0.132 point-to-point
 pvc 1/32
 encapsulation aal5snap
!
ipv6 address 2001:0DB8:2222::72/32
```

Cisco 2 Configuration

```

interface ATM0
  no ip address
!
interface ATM0.132 point-to-point
  pvc 1/32
    encapsulation aal5snap
  !
  ipv6 address 2001:0DB8:2222::45/32

```

In the following example, the same two nodes (Cisco 1 and Cisco 2) from the previous example are connected by the same PVC. In this example, however, the point-to-multipoint interface ATM0 is used on both nodes to terminate the PVC; therefore, explicit mappings are required between the link-local and global IPv6 addresses of interface ATM0 on both nodes and the PVC. Additionally, ATM pseudobroadcasts are enabled on the link-local address of interface ATM0 on both nodes.

Cisco 1 Configuration

```

interface ATM0
  no ip address
  pvc 1/32
    protocol ipv6 2001:0DB8:2222::45
    protocol ipv6 FE80::60:2FA4:8291:2 broadcast
    encapsulation aal5snap
  !
  ipv6 address 2001:0DB8:2222::72/32

```

Cisco 2 Configuration

```

interface ATM0
  no ip address
  pvc 1/32
    protocol ipv6 FE80::60:3E47:AC8:C broadcast
    protocol ipv6 2001:0DB8:2222::72
    encapsulation aal5snap
  !
  ipv6 address 2001:0DB8:2222::45/32

```

Related Commands

| Command | Description |
|---------------------|---|
| show atm map | Displays the list of all configured ATM static maps to remote hosts on an ATM network and on ATM bundle maps. |

redistribute (IPv6)

To redistribute IPv6 routes from one routing domain into another routing domain, use the **redistribute** command in address family configuration or router configuration mode. To disable redistribution, use the **no** form of this command.

redistribute *protocol* [*process-id*] [**level-1** [**into level-2**] | **level-1-2** | **level-2** [**into level-1**]]
[**metric** *metric-value*] [**metric-type** {**internal** | **external**}] [**route-map** *map-name*]

no redistribute *protocol* [*process-id*] [**level-1** [**into level-2**] | **level-1-2** | **level-2** [**into level-1**]]
[**metric** *metric-value*] [**metric-type** {**internal** | **external**}] [**route-map** *map-name*]

Syntax Description

| | |
|--|--|
| <i>protocol</i> | Source protocol from which routes are being redistributed. It can be one of the following keywords: bgp , connected , isis , rip , or static . The static keyword is used to redistribute IP static routes. The connected keyword refers to routes that are established automatically by virtue of IPv6 having been enabled on an interface. For routing protocols such as Intermediate System-to-Intermediate System (IS-IS), these routes will be redistributed as external to the autonomous system. |
| <i>process-id</i> | (Optional) For the bgp keyword, this is a Border Gateway Protocol (BGP) autonomous system number, which is a 16-bit decimal number. For the isis keyword, this is an optional <i>tag</i> value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing. For the rip keyword, this is an optional <i>tag</i> value that defines a meaningful name for an IPv6 Routing Information Protocol (RIP) routing process. |
| level-1 [into level-2] | (Optional) Specifies that IS-IS Level 1 routes are redistributed into other IP routing protocols independently. To distribute IS-IS Level 1 routes into Level 2 in another IS-IS instance, use the optional into level-2 keywords. |
| level-1-2 | (Optional) Specifies that IS-IS both Level 1 and Level 2 routes are redistributed into other IP routing protocols. |
| level-2 [into level-1] | (Optional) Specifies that IS-IS Level 2 routes are redistributed into other IP routing protocols independently. To distribute IS-IS Level 2 routes into Level 1 in another IS-IS instance, use the optional into level-1 keywords. |
| metric <i>metric-value</i> | (Optional) Metric used for the redistributed route. If a value is not specified for this option, and no value is specified using the default-metric command, the default metric value is 0. Use a value consistent with the destination protocol. |

| | |
|--|---|
| metric-type { internal external } | (Optional) For IS-IS, the external link type associated with the default route advertised into the IS-IS routing domain. The link type can be one of two values: <ul style="list-style-type: none"> • internal—IS-IS metric that is < 63. • external—IS-IS metric that is > 64 < 128. The default is internal . |
| route-map | (Optional) Route map that should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. If this keyword is not specified, all routes are redistributed. If this keyword is specified, but no route map names are listed, no routes are imported. |
| <i>map-name</i> | (Optional) Identifier of a configured route map. |

Defaults

Route redistribution is disabled.

protocol: No source protocol is defined.

process-id: No process ID is defined.

metric *metric-value*: 0.

metric-type **internal** | **external**: Internal.

route-map *map-name*: If the **route-map** keyword is not entered, all routes are redistributed; if no *map-name* value is entered, no routes are imported.

Command Modes

Address family configuration
Router configuration

Command History

| Release | Modification |
|------------|---|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was implemented on the Cisco 12000 series Internet routers, and support for IS-IS was added. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

A router receiving an IPv6 IS-IS route with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

IS-IS will ignore any configured redistribution of routes configured with the **connected** keyword. IS-IS will advertise a prefix on an interface if either IS-IS is running over the interface or the interface is configured as passive.

Routes learned from IPv6 routing protocols can be redistributed into IPv6 IS-IS at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

For IPv6 RIP use the **redistribute** (IPv6) command to advertise static routes as if they were directly connected routes.

**Caution**

Advertising static routes as directly connected routes can cause routing loops if improperly configured.

Redistributed IPv6 RIP routing information should always be filtered by the **distribute-list prefix-list** (IPv6 RIP) router configuration command. Use of the **distribute-list prefix-list** (IPv6 RIP) command ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

**Note**

The **metric** value specified in the **redistribute** command for IPv6 RIP supersedes the **metric** value specified using the **default-metric** command.

Examples

The following example configures IPv6 IS-IS to redistribute IPv6 BGP routes. The metric is specified as 5, and the metric type will be set to external, indicating that it has lower priority than internal metrics.

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# redistribute bgp 64500 metric 5 metric-type external
```

The following example redistributes IPv6 BGP routes into the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-rtr-rip)# redistribute bgp
```

Related Commands

| Command | Description |
|---|--|
| default-metric | Specifies a default metric for redistributed routes. |
| distribute-list prefix-list (IPv6 RIP) | Applies a prefix list to IPv6 RIP routing updates that are received or sent on an interface. |

remark (IPv6)

To write a helpful comment (remark) for an entry in an IPv6 access list, use the **remark** command in IPv6 access list configuration mode. To remove the remark, use the **no** form of this command.

remark *text-string*

no remark *text-string*

| | | |
|---------------------------|--------------------|--|
| Syntax Description | <i>text-string</i> | Comment that describes the access list entry, up to 100 characters long. |
|---------------------------|--------------------|--|

| | |
|-----------------|---|
| Defaults | IPv6 access list entries have no remarks. |
|-----------------|---|

| | |
|----------------------|--------------------------------|
| Command Modes | IPv6 access list configuration |
|----------------------|--------------------------------|

| Command History | Release | Modification |
|------------------------|-----------|---|
| | 12.0(23)S | This command was introduced. |
| | 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

| | |
|-------------------------|--|
| Usage Guidelines | The remark (IPv6) command is similar to the remark (IP) command, except that it is IPv6-specific. The remark can be up to 100 characters long; anything longer is truncated. |
|-------------------------|--|

| | |
|-----------------|--|
| Examples | The following example configures a remark for the IPv6 access list named TELNETTING. The remark is specific to not letting the Marketing subnet use outbound Telnet. |
|-----------------|--|

```
ipv6 access-list TELNETTING
remark Do not allow Marketing subnet to telnet out
deny tcp 2001:0DB8:0300:0201::/64 any eq telnet
```

| Related Commands | Command | Description |
|-------------------------|------------------------------|---|
| | ipv6 access-list | Defines an IPv6 access list and enters IPv6 access list configuration mode. |
| | show ipv6 access-list | Displays the contents of all current IPv6 access lists. |

set dscp

To mark a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte, use the **set dscp** command in policy-map class configuration mode. To remove a previously set DSCP value, use the **no** form of this command.

```
set [ip] dscp {dscp-value | from-field [table table-map-name]}

no set [ip] dscp {dscp-value | from-field [table table-map-name]}
```

| | | |
|--------------------|----------------|---|
| Syntax Description | ip | (Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets. |
| | dscp-value | A number from 0 to 63 that sets the DSCP value. The following reserved keywords can be specified instead of numeric values: <ul style="list-style-type: none">• EF (expedited forwarding)• AF11 (assured forwarding class AF11)• AF12 (assured forwarding class AF12) |
| | from-field | Specific packet-marking category to be used to set the DSCP value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the “map from” packet-marking category. Packet-marking category keywords are as follows: <ul style="list-style-type: none">• cos• qos-group |
| | table | (Optional) Used in conjunction with the <i>from-field</i> argument. Indicates that the values set in a specified table map will be used to set the DSCP value. |
| | table-map-name | (Optional) Used in conjunction with the table keyword. Name of the table map used to specify the DSCP value. The name can be a maximum of 64 alphanumeric characters. |

Defaults Disabled

Command Modes Policy-map class configuration

| | | |
|-----------------|-----------|--|
| Command History | Release | Modification |
| | 12.2(13)T | This command was introduced. This command replaces the set ip dscp command. |

Usage Guidelines Once the DSCP bit is set, other quality of service (QoS) features can then operate on the bit settings.

DSCP and Precedence Values Are Mutually Exclusive

The **set dscp** command cannot be used with the **set precedence** command to mark the *same* packet. The two values, DSCP and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

Precedence Value and Queueing

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the precedence. Weighted fair queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Use of the “from-field” Packet-marking Category

If you are using this command as part of the Enhanced Packet Marking feature, you can use this command to specify the “from-field” packet-marking category to be used for mapping and setting the DSCP value. The “from-field” packet-marking categories are as follows:

- Class of service (CoS)
- QoS group

If you specify a “from-field” category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the “from-field” category as the DSCP value. For instance, if you configure the **set dscp cos** command, the CoS value will be copied and used as the DSCP value.



Note

The CoS field is a three-bit field, and the DSCP field is a six-bit field. If you configure the **set dscp cos** command, only the three bits of the CoS field will be used.

If you configure the **set dscp qos-group** command, the QoS group value will be copied and used as the DSCP value.

The valid value range for the DSCP is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **set dscp qos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value will be copied and the packets will be marked.
- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value will not be copied and the packet will not be marked. No action is taken.

Set DSCP Values in IPv6 Environments

When this command is used in IPv6 environments, the default match occurs on both IP and IPv6 packets. However, the actual packets set by this function are only those which meet the match criteria of the class-map containing this function.

Set DSCP Values for IPv6 Packets Only

To set DSCP values for IPv6 values only, the **match protocol ipv6** command must also be used. Without that command, the precedence match defaults to match both IPv4 and IPv6 packets.

Set DSCP Values for IPv4 Packets Only

To set DSCP values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword the match occurs on both IPv4 and IPv6 packets.

Examples

Packet-marking Values and Table Map

In the following example, the policy map called “policy1” is created to use the packet-marking values defined in a table map called “table-map1”. The table map was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the table-map (value mapping) command page.

In this example, the DSCP value will be set according to the CoS value defined in the table map called “table-map1”.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set dscp cos table table-map1
Router(config-pmap-c)# exit
```

The **set dscp** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface. For information on attaching a service policy to an interface, refer to the “Modular Quality of Service Command-Line Interface” section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Related Commands

| Command | Description |
|----------------------------------|--|
| policy-map | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| service-policy | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| set cos | Sets the Layer 2 CoS value of an outgoing packet. |
| set precedence | Sets the precedence value in the packet header. |
| show policy-map | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| show policy-map class | Displays the configuration for the specified class of the specified policy map. |
| show policy-map interface | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |
| show table-map | Displays the configuration of a specified table map or all table maps. |
| table-map (value mapping) | Creates and configures a mapping table for mapping and converting one packet-marking value to another. |

set ipv6 next-hop (BGP)

To indicate where to output IPv6 packets that pass a match clause of a route map for policy routing, use the **set ipv6 next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ipv6 next-hop *ipv6-address* [*link-local-address*]

no set ipv6 next-hop *ipv6-address* [*link-local-address*]

Syntax Description

| | |
|---------------------------|--|
| <i>ipv6-address</i> | IPv6 global address of the next hop to which packets are output. It need not be an adjacent router. 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>link-local-address</i> | (Optional) IPv6 link-local address of the next hop to which packets are output. It must be an adjacent router. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |

Defaults

Disabled

Command Modes

Route-map configuration

Command History

| Release | Modification |
|------------|--|
| 12.2(4)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **set ipv6 next-hop** command is similar to the **set ip next-hop** command, except that it is IPv6-specific.

The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

When the **set ipv6 next-hop** command is used with the **peer-address** keyword in an inbound route map of a BGP peer, the next hop of the received matching routes will be set to be the neighbor peering address, overriding any third-party next hops. So the same route map can be applied to multiple BGP peers to override third-party next hops.

When the **set ipv6 next-hop** command is used with the **peer-address** keyword in an outbound route map of a BGP peer, the next hop of the advertised matching routes will be set to be the peering address of the local router, thus disabling the next hop calculation. The **set ipv6 next-hop** command has finer

granularity than the per-neighbor **neighbor next-hop-self** command, because you can set the next hop for some routes, but not others. The **neighbor next-hop-self** command sets the next hop for all routes sent to that neighbor.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ipv6 next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

Examples

The following example configures the IPv6 multiprotocol BGP peer FE80::250:BFF:FE0E:A471 and sets the route map named nh6 to include the IPv6 next hop global addresses of Fast Ethernet interface 0 of the neighbor in BGP updates. The IPv6 next hop link-local address can be sent to the neighbor by the nh6 route map or from the interface specified by the **neighbor update-source** router configuration command.

```
router bgp 170
 neighbor FE80::250:BFF:FE0E:A471 remote-as 150
 neighbor FE80::250:BFF:FE0E:A471 update-source fastether 0

address-family ipv6
 neighbor FE80::250:BFF:FE0E:A471 activate
 neighbor FE80::250:BFF:FE0E:A471 route-map nh6 out

route-map nh6
 set ipv6 next-hop 3FFE:506::1
```



Note

If you specify only the global IPv6 next hop address (the *ipv6-address* argument) with the **set ipv6 next-hop** command after specifying the neighbor interface (the *interface-type* argument) with the **neighbor update-source** command, the link-local address of the neighbor interface is included as the next hop in the BGP updates. Therefore, only one route map that sets the global IPv6 next hop address in BGP updates is required for multiple BGP peers that use link-local addresses.

Related Commands

| Command | Description |
|--------------------------------|---|
| ip policy route-map | Identifies a route map to use for policy routing on an interface. |
| match ipv6 address | Distributes IPv6 routes that have a prefix permitted by a prefix list. |
| match ipv6 next-hop | Distributes IPv6 routes that have a next hop prefix permitted by a prefix list. |
| match ipv6 route-source | Distributes IPv6 routes that have been advertised by routers at an address specified by a prefix list. |
| neighbor next-hop-self | Disables next-hop processing of BGP updates on the router. |
| neighbor update-source | Specifies that the Cisco IOS software allow BGP sessions to use any operational interface for TCP connections |
| route-map (IP) | Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing. |

set precedence

To set the precedence value in the packet header, use the **set precedence** command in policy-map class configuration mode. To remove the precedence value, use the **no** form of this command.

set precedence {*precedence-value* | *from-field* [**table** *table-map-name*]}

no set precedence {*precedence-value* | *from-field* [**table** *table-map-name*]}

| | | |
|---------------------------|-------------------------|--|
| Syntax Description | <i>precedence-value</i> | A number from 0 to 7 that sets the precedence bit in the packet header. |
| | <i>from-field</i> | Specific packet-marking category to be used to set the precedence value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the “map from” packet-marking category. Packet-marking category keywords are as follows: <ul style="list-style-type: none"> • cos • qos-group |
| | table | (Optional) Used in conjunction with the <i>from-field</i> argument. Indicates that the values set in a specified table map will be used to set the precedence value. |
| | <i>table-map-name</i> | (Optional) Used in conjunction with the table keyword. Name of the table map used to specify a precedence value based on the class of service (CoS) value. The name can be a maximum of 64 alphanumeric characters. |
| | | |

Defaults Disabled

Command Modes Policy-map class configuration

| | | |
|------------------------|----------------|--|
| Command History | Release | Modification |
| | 12.2(13)T | This command was introduced. This command replaces the set ip precedence command. |

Usage Guidelines

Command Compatibility

If a router is loaded with an image from this version that contained old configuration, the **set ip precedence** command is still recognized. However, commands like **show running-configuration**, **write memory**, **copy running-configuration xxx** will generate **set precedence** in place of **set ip precedence** that existed earlier.

The **set precedence** command cannot be used with the **set dscp** command to mark the *same* packet. The two values, DSCP and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

Bit Settings

Once the precedence bits are set, other quality of service (QoS) features such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) then operate on the bit settings.

Precedence Value

The network gives priority (or some type of expedited handling) to marked traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the specified precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during times of congestion.

Use of the “from-field” Packet-marking Category

You can use this command to specify the “from-field” packet-marking category to be used for mapping and setting the precedence value. The “from-field” packet-marking categories are as follows:

- Class of service (CoS)
- QoS group

If you specify a “from-field” category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the “from-field” category as the precedence value. For instance, if you configure the **set precedence cos** command, the CoS value will be copied and used as the precedence value.

You can do the same for the QoS group-marking category. That is, you can configure the **set precedence qos-group** command, and the QoS group value will be copied and used as the precedence value.

The valid value range for the precedence value is a number from 0 to 7. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **set precedence qos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 6), the packet-marking value will be copied and the packets will be marked.
- If QoS group value exceeds the precedence range (for example, 10), the packet-marking value will not be copied, and the packet will not be marked. No action is taken.

Precedence Values in IPv6 Environments

When this command is used in IPv6 environments it can set the value in both IPv4 and IPv6 packets. However, the actual packets set by this function are only those that meet the match criteria of the class-map containing this function.

Set Precedence Values for IPv6 Packets Only

To set precedence values for IPv6 packets only, the **match protocol ipv6** command must also be used in the class-map that classified packets for this action. Without that command, the class-map may classify both IPv6 and IPv4 packets, (depending on other match criteria) and **set precedence** will act upon both of them.

Set Precedence Values for IPv4 Packets Only

To set precedence values for IPv4 packets only, use the a command involving **ip** keyword like **match ip dscp** or include the **match protocol ip** command along with the others in the class-map. Without that, the class-map may match both IPv6 and IPv4 packets, (depending on other match criteria) and **set dscp** may act upon both of them.

Examples

In the following example, the policy map called “policy-cos” is created to use the values defined in a table map called “table-map1”. The table map called “table-map1” was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the table-map (value mapping) command page.

In this example, the precedence value will be set according to the CoS value defined in “table-map1”.

```
Router(config)# policy-map policy-cos
Router(config-pmap)# class class-default
Router(config-pmap-c)# set precedence cos table table-map1
Router(config-pmap-c)# exit
```

The **set precedence** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface or to an ATM virtual circuit. For information on attaching a service policy to an interface, refer to the “Modular Quality of Service Command-Line Interface” section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Related Commands

| Command | Description |
|----------------------------------|---|
| policy-map | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| service-policy | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| set cos | Sets the Layer 2 CoS value of an outgoing packet. |
| set dscp | Marks a packet by setting the Layer 3 DSCP value in the ToS byte. |
| set qos-group | Sets a group ID that can be used later to classify packets. |
| show policy-map | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| show policy-map interface | Displays the configuration for all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |
| show table-map | Displays the configuration of a specified table map or all table maps. |
| table-map (value mapping) | Creates and configures a mapping table for mapping and converting one packet-marking value to another. |

show atm map

To display the list of all configured ATM static maps to remote hosts on an ATM network and on ATM bundle maps, use the **show atm map** command in EXEC mode.

show atm map

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

| | |
|----------------------|------|
| Command Modes | EXEC |
|----------------------|------|

| Command History | Release | Modification |
|-----------------|--|--|
| | 10.0 | This command was introduced. |
| | 11.1 CA | This command was modified to include an example for the ATM-CES port adapter (PA). |
| | 12.0(3)T | This command was modified to include display for ATM bundle maps. An ATM bundle map identifies a bundle and all of its related virtual circuits (VCs). |
| | 12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S | The display output for this command was modified to include the IPv6 address mappings of remote nodes to ATM permanent virtual circuits (PVCs). |

Examples

The following is sample output from the **show atm map** command for a bundle called san-jose (0/122, 0/123, 0/124, and 0/126 are the virtual path and virtual channel identifiers of the bundle members):

```
Router# show atm map

Map list san-jose_B_ATM1/0.52 : PERMANENT
ip 10.1.1.1. maps to bundle san-jose, 0/122, 0/123, 0/124, 0/126, ATM1/0.52, broadcast
```

The following is sample output from the **show atm map** command for an ATM-CES PA on the Cisco 7200 series router:

```
Router# show atm map

Map list alien: PERMANENT
ip 10.1.1.1 maps to VC 6
ip 10.1.1.2 maps to VC 6
```

The following is sample output from the **show atm map** command that displays information for a bundle called new-york:

```
Router# show atm map

Map list atm:
vines 3004B310:0001 maps to VC 4, broadcast
ip 172.21.168.110 maps to VC 1, broadcast
clns 47.0004.0001.0000.0c00.6e26.00 maps to VC 6, broadcast
appletalk 10.1 maps to VC 7, broadcast
```

```
decnet 10.1 maps to VC 2, broadcast
Map list new-york: PERMANENT
ip 10.0.0.2 maps to bundle new-york, 0/200, 0/205, 0/210, ATM1/0.1
```

The following is sample output from the **show atm map** command for a multipoint connection:

```
Router# show atm map

Map list atm_pri: PERMANENT
ip 10.4.4.4 maps to NSAP CD.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12, broadcast,
aal5mux, multipoint connection up, VC 6
ip 10.4.4.6 maps to NSAP DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12, broadcast,
aal5mux, connection up, VC 15, multipoint connection up, VC 6

Map list atm_ipx: PERMANENT
ipx 1004.dddd.dddd.dddd maps to NSAP DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12,
broadcast, aal5mux, multipoint connection up, VC 8
ipx 1004.cccc.cccc.cccc maps to NSAP CD.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12,
broadcast, aal5mux, multipoint connection up, VC 8

Map list atm_apple: PERMANENT
appletalk 62000.5 maps to NSAP CD.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12,
broadcast, aal5mux, multipoint connection up, VC 4
appletalk 62000.6 maps to NSAP DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12,
broadcast, aal5mux, multipoint connection up, VC 4
```

The following is sample output from the **show atm map** command if you configure an ATM PVC using the **pvc** command:

```
Router# show atm map

Map list endA: PERMANENT
ip 10.11.11.1 maps to VC 4, VPI 0, VCI 60, ATM0.2
```

The following sample output from the **show atm map** command shows the link-local and global IPv6 addresses (FE80::60:3E47:AC8:C and 2001:0DB8:2222::72, respectively) of a remote node that are explicitly mapped to PVC 1/32 of ATM interface 0;

```
Router# show atm map

Map list ATM0pvc1 : PERMANENT
ipv6 FE80::60:3E47:AC8:C maps to VC 1, VPI 1, VCI 32, ATM0
, broadcast
ipv6 2001:0DB8:2222::72 maps to VC 1, VPI 1, VCI 32, ATM0
```

Table 24 describes the significant fields shown in the displays.

Table 24 *show atm map Field Descriptions*

| Field | Description |
|--|--|
| Map list | Name of map list. |
| PERMANENT | This map entry was entered from configuration; it was not entered automatically by a process. |
| ip 172.21.168.110 maps to VC 1 or ip 10.4.4.6 maps to NSAP DE.CDEF.01.234567.890A.BCDE.F012.345 6.7890.1234.12 | Name of protocol, the protocol address, and the virtual circuit descriptor (VCD) or network service access point (NSAP) to which the address is mapped (for ATM VCs configured with the atm pvc command). |
| broadcast | Indicates pseudobroadcasting. |

Table 24 *show atm map Field Descriptions (continued)*

| Field | Description |
|---|--|
| ip 10.11.11.1 maps to VC 4, VPI 0, VCI 60, ATM0.2 | Name of protocol, the protocol address, the virtual path identifier (VPI) number, the virtual channel identifier (VCI) number, and the ATM interface or subinterface (for ATM PVCs configured using the pvc command). |
| or | or |
| ip 10.4.4.6 maps to NSAP DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12 | Name of the protocol, the protocol address, and the NSAP to which the address is mapped (for ATM switched virtual circuits (SVCs) configured using the svc command). |
| aal5mux | Indicates the encapsulation used, a multipoint or point-to-point VC, and the number of the virtual circuit. |
| multipoint connection up | Indicates that this is a multipoint VC. |
| VC 6 | Number of the VC. |
| connection up | Indicates a point-to-point VC. |
| VPI | VPI for the VC. |
| VCI | VCI for the VC. |
| ATM1/0.52 | ATM interface or subinterface number. |
| Map list | Name of the bundle whose mapping information follows. |
| ip 10.1.1.1 maps to bundle san-jose, 0/122, 0/123, 0/124, 0/126 | IP address of the bundle and VC members that belong to the bundle. |

Related Commands

| Command | Description |
|-----------------------------------|--|
| protocol (ATM) | Configures a static map for an ATM PVC, SVC, VC class, or VC bundle. Enables Inverse ARP or Inverse ARP broadcasts on an ATM PVC by either configuring Inverse ARP directly on the PVC, on the VC bundle, or in a VC class (applies to IP and IPX protocols only). |
| protocol ipv6 (ATM) | Maps the IPv6 address of a remote node to the ATM PVC used to reach the address. |
| pvc | Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, or enters interface-ATM-VC configuration mode. |
| show atm bundle | Displays the bundle attributes assigned to each bundle VC member and the current working status of the VC members. |
| show atm bundle statistics | Displays statistics on the specified bundle. |
| svc | Creates an ATM SVC and specifies destination NSAP address on an interface or subinterface. |

show bgp ipv6

To display entries in the IPv6 Border Gateway Protocol (BGP) routing table, use the **show bgp ipv6** command in user EXEC or privileged EXEC mode.

show bgp ipv6 [*ipv6-prefix/prefix-length*] [**longer-prefixes**] [**labels**]

| | | |
|---------------------------|------------------------|--|
| Syntax Description | <i>ipv6-prefix</i> | (Optional) IPv6 network number, entered to display a particular network in the IPv6 BGP routing table. 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> | (Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |
| | longer-prefixes | (Optional) Displays the route and more specific routes. |
| | labels | (Optional) Displays Multiprotocol Label Switching (MPLS) label information. |

| | |
|----------------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | MPLS label information was added to the display. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| | 12.3(2)T | MPLS label value advertised for the IPv6 prefix was added to the display. |

| | |
|-------------------------|--|
| Usage Guidelines | The show bgp ipv6 command provides output similar to the show ip bgp command, except that it is IPv6-specific. |
|-------------------------|--|

Examples

The following is sample output from the **show bgp ipv6** command:

```
Router# show bgp ipv6
```

```
BGP table version is 12612, local router ID is 172.16.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

| Network | Next Hop | Metric | LocPrf | Weight | Path |
|-------------------|---------------------|--------|--------|--------|-----------------------|
| * | 3FFE:C00:E:C::2 | | | 0 | 3748 4697 1752 i |
| * | 3FFE:1100:0:CC00::1 | | | 0 | 1849 1273 1752 i |
| * 2001:618:3::/48 | 3FFE:C00:E:4::2 | 1 | | 0 | 4554 1849 65002 i |
| *> | 3FFE:1100:0:CC00::1 | | | 0 | 1849 65002 i |
| * 2001:620::/35 | 2001:0DB8:0:F004::1 | | | 0 | 3320 1275 559 i |
| * | 3FFE:C00:E:9::2 | | | 0 | 1251 1930 559 i |
| * | 3FFE:3600::A | | | 0 | 3462 10566 1930 559 i |
| * | 3FFE:700:20:1::11 | | | 0 | 293 1275 559 i |
| * | 3FFE:C00:E:4::2 | 1 | | 0 | 4554 1849 1273 559 i |
| * | 3FFE:C00:E:B::2 | | | 0 | 237 3748 1275 559 i |

Table 25 describes the significant fields shown in the display.

Table 25 show bgp ipv6 Field Descriptions

| Field | Description |
|-------------------|---|
| BGP table version | Internal version number of the table. This number is incremented whenever the table changes. |
| local router ID | A 32-bit number written as 4 octets separated by periods (dotted decimal format). |
| Status codes | Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP session. |
| Origin codes | Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from the Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP. |
| Network | IPv6 address of a network entity. |

Table 25 *show bgp ipv6 Field Descriptions (continued)*

| Field | Description |
|----------|--|
| Next Hop | IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network. |
| Metric | If shown, this is the value of the interautonomous system metric. |
| LocPrf | Local preference value as set with the set local-preference route-map configuration command. The default value is 100. |
| Weight | Weight of the route as set via autonomous system filters. |
| Path | Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. |

The following is sample output from the **show bgp ipv6** command, showing information for prefix 3FFE:500::/24:

```
Router# show bgp ipv6 3FFE:500::/24

BGP routing table entry for 3FFE:500::/24, version 19421
Paths: (6 available, best #1)
  Advertised to peer-groups:
    6BONE
  293 3425 2500
    3FFE:700:20:1::11 from 3FFE:700:20:1::11 (192.168.2.27)
      Origin IGP, localpref 100, valid, external, best
  4554 293 3425 2500
    3FFE:C00:E:4::2 from 3FFE:C00:E:4::2 (192.168.1.1)
      Origin IGP, metric 1, localpref 100, valid, external
  33 293 3425 2500
    3FFE:C00:E:5::2 from 3FFE:C00:E:5::2 (209.165.18.254)
      Origin IGP, localpref 100, valid, external
      Dampinfo: penalty 673, flapped 429 times in 10:47:45
  6175 7580 2500
    3FFE:C00:E:1::2 from 3FFE:C00:E:1::2 (209.165.223.204)
      Origin IGP, localpref 100, valid, external
  1849 4697 2500, (suppressed due to dampening)
    3FFE:1100:0:CC00::1 from 3FFE:1100:0:CC00::1 (172.31.38.102)
      Origin IGP, localpref 100, valid, external
      Dampinfo: penalty 3938, flapped 596 times in 13:03:06, reuse in 00:59:10
  237 10566 4697 2500
    3FFE:C00:E:B::2 from 3FFE:C00:E:B::2 (172.31.0.3)
      Origin IGP, localpref 100, valid, external
```

The following is sample output from the **show bgp ipv6** command, showing MPLS label information for an IPv6 prefix that is configured to be an IPv6 edge router using MPLS:

```
Router# show bgp ipv6 2001:0DB8::/32

BGP routing table entry for 2001:0DB8::/32, version 15
Paths: (1 available, best #1)
  Not advertised to any peer
  Local
    ::FFFF:192.168.99.70 (metric 20) from 192.168.99.70 (192.168.99.70)
      Origin IGP, localpref 100, valid, internal, best, mpls label 17
```

To display the top of the stack label with label switching information, enter the **show bgp ipv6 EXEC** command with the **labels** keyword:

```
Router# show bgp ipv6 labels
```

```
Network                Next Hop                In tag/Out tag
2001:0DB8::/32         ::FFFF:192.168.99.70    notag/20
```



Note

If a prefix has not been advertised to any peer, the display shows “Not advertised to any peer.”

Related Commands

| Command | Description |
|--------------------------------------|---|
| clear bgp ipv6 | Resets an IPv6 BGP connection or session. |
| neighbor soft-reconfiguration | Configures the Cisco IOS software to start storing updates. |

show bgp ipv6 community

To display routes that belong to specified IPv6 Border Gateway Protocol (BGP) communities, use the **show bgp ipv6 community** command in user EXEC or privileged EXEC mode.

```
show bgp ipv6 {unicast | multicast} community [community-number] [exact-match] [local-as |
no-advertise | no-export]
```

| | | |
|---------------------------|-------------------------|---|
| Syntax Description | unicast | Specifies IPv6 unicast address prefixes. |
| | multicast | Specifies IPv6 multicast address prefixes. |
| | <i>community-number</i> | (Optional) Valid value is a community number in the range from 1 to 4294967295 or AA:NN (autonomous system-community number:2-byte number). |
| | exact-match | (Optional) Displays only routes that have an exact match. |
| | local-as | (Optional) Displays only routes that are not sent outside of the local autonomous system (well-known community). |
| | no-advertise | (Optional) Displays only routes that are not advertised to any peer (well-known community). |
| | no-export | (Optional) Displays only routes that are not exported outside of the local autonomous system (well-known community). |

| | |
|----------------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| | 12.3(2)T | The unicast and exact-match keywords were added. |
| | 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines The **show bgp ipv6 community** and the **show bgp ipv6 community** commands provide output similar to the **show ip bgp community** command, except they are IPv6-specific.

Communities are set with the **set community** route-map configuration command. You must enter the numerical communities before the well-known communities. For example, the following string is not valid:

```
Router# show ipv6 bgp community local-as 111:12345
```

Use one of the following strings instead:

```
Router# show ipv6 bgp community 111:12345 local-as
```

```
Router# show ipv6 bgp unicast community 111:12345 local-as
```

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples



Note

The following is sample output from the **show bgp ipv6 community** command:

The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
BGP table version is 69, local router ID is 10.2.64.5
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
```

| Network | Next Hop | Metric | LocPrf | Weight | Path |
|-------------------------|------------------|--------|--------|--------|---------|
| *> 2001:0DB8:0:1::1/64 | :: | | | 0 | 32768 i |
| *> 2001:0DB8:0:1:1::/80 | :: | | | 0 | 32768 ? |
| *> 2001:0DB8:0:2::/64 | 2001:0DB8:0:3::2 | | | 0 | 2 i |
| *> 2001:0DB8:0:2:1::/80 | 2001:0DB8:0:3::2 | | | 0 | 2 ? |
| * 2001:0DB8:0:3:1/64 | 2001:0DB8:0:3::2 | | | 0 | 2 ? |
| *> | :: | | | 0 | 32768 ? |
| *> 2001:0DB8:0:4::/64 | 2001:0DB8:0:3::2 | | | 0 | 2 ? |
| *> 2001:0DB8:0:5:1/64 | :: | | | 0 | 32768 ? |
| *> 2001:0DB8:0:6::/64 | 2000:0:0:3::2 | | | 0 | 2 3 i |
| *> 2010::/64 | :: | | | 0 | 32768 ? |
| *> 2020::/64 | :: | | | 0 | 32768 ? |
| *> 2030::/64 | :: | | | 0 | 32768 ? |
| *> 2040::/64 | :: | | | 0 | 32768 ? |
| *> 2050::/64 | :: | | | 0 | 32768 ? |

Table 26 describes the significant fields shown in the display.

Table 26 show bgp ipv6 community Field Descriptions

| Field | Description |
|-------------------|--|
| BGP table version | Internal version number of the table. This number is incremented whenever the table changes. |
| local router ID | A 32-bit number written as 4 octets separated by periods (dotted-decimal format). |

Table 26 *show bgp ipv6 community Field Descriptions (continued)*

| Field | Description |
|--------------|--|
| Status codes | <p>Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values:</p> <p>s—The table entry is suppressed.</p> <p>d—The table entry is dampened.</p> <p>h—The table entry is history.</p> <p>*—The table entry is valid.</p> <p>>—The table entry is the best entry to use for that network.</p> <p>i—The table entry was learned via an internal BGP session.</p> |
| Origin codes | <p>Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values:</p> <p>i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a network router configuration command.</p> <p>e—Entry originated from the Exterior Gateway Protocol (EGP).</p> <p>?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.</p> |
| Network | IPv6 address of a network entity. |
| Next Hop | IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network. |
| Metric | The value of the interautonomous system metric. This field is frequently not used. |
| LocPrf | Local preference value as set with the set local-preference route-map configuration command. The default value is 100. |
| Weight | Weight of the route as set via autonomous system filters. |
| Path | Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. |

Related Commands

| Command | Description |
|--------------------------------------|--|
| clear bgp ipv6 | Resets an IPv6 BGP connection or session. |
| ip bgp-community new-format | Displays BGP communities in the format AA:NN (autonomous system-community number:2-byte number). |
| neighbor soft-reconfiguration | Configures the Cisco IOS software to start storing updates. |

show bgp ipv6 community-list

To display routes that are permitted by the IPv6 Border Gateway Protocol (BGP) community list, use the **show bgp ipv6 community-list** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {unicast | multicast} community-list {number | name} [exact-match]

Syntax Description

| | |
|--------------------|---|
| unicast | Specifies IPv6 unicast address prefixes. |
| multicast | Specifies IPv6 multicast address prefixes. |
| <i>number</i> | Community list number in the range from 1 to 199. |
| <i>name</i> | Community list name. |
| exact-match | (Optional) Displays only routes that have an exact match. |

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|------------|---|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.3(2)T | The unicast keyword was added. |
| 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines

The **show bgp ipv6 community-list** and **show bgp ipv6 unicast community-list** commands provide output similar to the **show ip bgp community-list** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output of the **show bgp ipv6 community-list** command for community list number 3:

**Note**

The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast community-list 3
```

```
BGP table version is 14, local router ID is 10.2.64.6
```

```
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
```

```
Origin codes:i - IGP, e - EGP, ? - incomplete
```

| Network | Next Hop | Metric | LocPrf | Weight | Path |
|-------------------------|------------------|--------|--------|--------|---------|
| *> 2001:0DB8:0:1::/64 | 2001:0DB8:0:3::1 | | | 0 | 1 i |
| *> 2001:0DB8:0:1:1::/80 | 2001:0DB8:0:3::1 | | | 0 | 1 i |
| *> 2001:0DB8:0:2::1/64 | :: | | | 0 | 32768 i |
| *> 2001:0DB8:0:2:1::/80 | :: | | | 0 | 32768 ? |
| * 2001:0DB8:0:3::2/64 | 2001:0DB8:0:3::1 | | | 0 | 1 ? |
| *> | :: | | | 0 | 32768 ? |
| *> 2001:0DB8:0:4::2/64 | :: | | | 0 | 32768 ? |
| *> 2001:0DB8:0:5::/64 | 2001:0DB8:0:3::1 | | | 0 | 1 ? |
| *> 2010::/64 | 2001:0DB8:0:3::1 | | | 0 | 1 ? |
| *> 2020::/64 | 2001:0DB8:0:3::1 | | | 0 | 1 ? |
| *> 2030::/64 | 2001:0DB8:0:3::1 | | | 0 | 1 ? |
| *> 2040::/64 | 2001:0DB8:0:3::1 | | | 0 | 1 ? |
| *> 2050::/64 | 2001:0DB8:0:3::1 | | | 0 | 1 ? |

Table 27 describes the significant fields shown in the display.

Table 27 *show bgp ipv6 community-list Field Descriptions*

| Field | Description |
|-------------------|---|
| BGP table version | Internal version number of the table. This number is incremented whenever the table changes. |
| local router ID | A 32-bit number written as 4 octets separated by periods (dotted-decimal format). |
| Status codes | Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP session. |
| Origin codes | Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from the Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP. |

Table 27 *show bgp ipv6 community-list Field Descriptions (continued)*

| Field | Description |
|----------|--|
| Network | IPv6 address of a network entity. |
| Next Hop | IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network. |
| Metric | The value of the interautonomous system metric. This field is frequently not used. |
| LocPrf | Local preference value as set with the set local-preference route-map configuration command. The default value is 100. |
| Weight | Weight of the route as set via autonomous system filters. |
| Path | Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. |

Related Commands

| Command | Description |
|--------------------------------------|---|
| clear bgp ipv6 | Resets an IPv6 BGP connection or session. |
| neighbor soft-reconfiguration | Configures the Cisco IOS software to start storing updates. |

show bgp ipv6 dampened-paths

To display IPv6 Border Gateway Protocol (BGP) dampened routes, use the **show bgp ipv6 dampened-paths** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {unicast | multicast} dampening dampened-paths

Syntax Description

| | |
|------------------|--|
| unicast | Specifies IPv6 unicast address prefixes. |
| multicast | Specifies IPv6 multicast address prefixes. |
| dampening | Displays detailed information about dampening. |

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|------------|---|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.3(2)T | The unicast and dampening keywords were added. |
| 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines

The **show bgp ipv6 dampened-paths** and **show bgp ipv6 unicast dampening dampened-paths** commands provide output similar to the **show ip bgp dampened-paths** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 dampened-paths** command:



Note

The command output is the same whether or not the **unicast**, **multicast**, and **dampening** keywords are used. The **unicast** and **dampening** keywords are available only in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast dampening dampened-paths
```

```
BGP table version is 12610, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```

      Network          From           Reuse      Path
*d 3FFE:1000::/24    3FFE:C00:E:B::2  00:00:10 237 2839 5609 i
*d 2001:228::/35    3FFE:C00:E:B::2  00:23:30 237 2839 5609 2713 i

```

Table 28 describes the significant fields shown in the display.

Table 28 *show bgp ipv6 dampened-paths Field Descriptions*

| Field | Description |
|-------------------|---|
| BGP table version | Internal version number of the table. This number is incremented whenever the table changes. |
| local router ID | A 32-bit number written as 4 octets separated by periods (dotted-decimal format). |
| Status codes | Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP session. |
| Origin codes | Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from the Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP. |
| Network | Indicates the network to which the route is dampened. |
| From | IPv6 address of the peer that advertised this path. |
| Reuse | Time (in hours:minutes:seconds) after which the path will be made available. |
| Path | Autonomous system path of the route that is being dampened. |

Related Commands

| Command | Description |
|---------------------------------|---|
| bgp dampening | Enables BGP route dampening or changes various BGP route dampening factors. |
| clear bgp ipv6 dampening | Clears IPv6 BGP route dampening information and unsuppresses the suppressed routes. |

show bgp ipv6 filter-list

To display routes that conform to a specified IPv6 filter list, use the **show bgp ipv6 filter-list** command in user EXEC or privileged EXEC mode.

show bgp ipv6 { unicast | multicast } filter-list *access-list-number*

| | | |
|---------------------------|---------------------------|---|
| Syntax Description | unicast | Specifies IPv6 unicast address prefixes. |
| | multicast | Specifies IPv6 multicast address prefixes. |
| | <i>access-list-number</i> | Number of an IPv6 autonomous system path access list. It can be a number from 1 to 199. |

| | |
|----------------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| | 12.3(2)T | The unicast keyword was added. |
| | 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines The **show bgp ipv6 filter-list** command provides output similar to the **show ip bgp filter-list** command, except that it is IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples The following is sample output from the **show bgp ipv6 filter-list** command for IPv6 autonomous system path access list number 1:



Note

The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast filter-list 1
```

```
BGP table version is 26, local router ID is 192.168.0.2
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
```

| Network | Next Hop | Metric | LocPrf | Weight | Path |
|-------------------------|------------------|--------|--------|--------|------|
| *> 2001:0DB8:0:1::/64 | 2001:0DB8:0:4::2 | | 0 | 2 1 i | |
| *> 2001:0DB8:0:1:1::/80 | 2001:0DB8:0:4::2 | | 0 | 2 1 i | |
| *> 2001:0DB8:0:2:1::/80 | 2001:0DB8:0:4::2 | | 0 | 2 ? | |
| *> 2001:0DB8:0:3::/64 | 2001:0DB8:0:4::2 | | 0 | 2 ? | |
| *> 2001:0DB8:0:4::/64 | :: | | 32768 | | ? |
| * | 2001:0DB8:0:4::2 | | 0 | 2 ? | |
| *> 2001:0DB8:0:5::/64 | :: | | 32768 | | ? |
| * | 2001:0DB8:0:4::2 | | 0 | 2 1 ? | |
| *> 2001:0DB8:0:6::1/64 | :: | | 32768 | | i |
| *> 2030::/64 | 2001:0DB8:0:4::2 | | 0 | 1 | |
| *> 2040::/64 | 2001:0DB8:0:4::2 | | 0 | 2 1 ? | |
| *> 2050::/64 | 2001:0DB8:0:4::2 | | 0 | 2 1 ? | |

Table 29 describes the significant fields shown in the display.

Table 29 show bgp ipv6 filter-list Field Descriptions

| Field | Description |
|-------------------|---|
| BGP table version | Internal version number for the table. This number is incremented any time the table changes. |
| local router ID | A 32-bit number written as 4 octets separated by periods (dotted-decimal format). |
| Status codes | Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP session. |
| Origin codes | Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP. |
| Network | IPv6 address of the network the entry describes. |
| Next Hop | IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network. |
| Metric | If shown, this is the value of the interautonomous system metric. This field is frequently not used. |

Table 29 *show bgp ipv6 filter-list Field Descriptions (continued)*

| Field | Description |
|--------|---|
| LocPrf | Local preference value as set with the set local-preference route-map configuration command. The default value is 100. |
| Weight | Weight of the route as set via autonomous system filters. |
| Path | <p>Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path. It can be one of the following values:</p> <p>i—The entry was originated with the IGP and advertised with a network router configuration command.</p> <p>e—The route originated with EGP.</p> <p>?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.</p> |

Related Commands

| Command | Description |
|-------------------------------|---|
| ip as-path access-list | Defines a BGP autonomous system path access list. |

show bgp ipv6 flap-statistics

To display IPv6 Border Gateway Protocol (BGP) flap statistics, use the **show bgp ipv6 flap-statistics** command in user EXEC or privileged EXEC mode.

```
show bgp ipv6 {unicast | multicast} dampening flap-statistics [regex regular-expression |
quote-regex regular-expression | filter-list list | ipv6-prefix/prefix-length [longer-prefix]]
```

| Syntax Description | | |
|---|--|---|
| unicast | | Specifies IPv6 unicast address prefixes. |
| multicast | | Specifies IPv6 multicast address prefixes. |
| dampening | | Displays detailed information about dampening. |
| regex <i>regular-expression</i> | | (Optional) Displays flap statistics for all the paths that match the regular expression. |
| quote-regex <i>regular-expression</i> | | (Optional) Displays flap statistics for all the paths that match the regular expression as a quoted string of characters. |
| filter-list <i>list</i> | | (Optional) Displays flap statistics for all the paths that pass the access list. |
| <i>ipv6-prefix</i> | | (Optional) Displays flap statistics for a single entry at this IPv6 network number. 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> | | (Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |
| longer-prefix | | (Optional) Displays flap statistics for more specific entries. |

| Command Modes | User EXEC Privileged EXEC |
|---------------|------------------------------|
|---------------|------------------------------|

| Command History | Release | Modification |
|-----------------|------------|---|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| | 12.3(2)T | The unicast and dampening keywords were added. |
| | 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

| Usage Guidelines | <p>The show bgp ipv6 flap-statistics and show bgp ipv6 unicast dampening flap-statistics commands provide output similar to the show ip bgp flap-statistics command, except they are IPv6-specific.</p> <p>If no arguments or keywords are specified, the router displays flap statistics for all routes.</p> |
|------------------|--|
|------------------|--|

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 flap-statistics** command without arguments or keywords:



Note

The output is the same whether or not the **unicast**, **multicast**, and **dampening** keywords are used. The **unicast** and **dampening** keywords are available only in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast dampening flap-statistics

BGP table version is 12612, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From          Flaps Duration Reuse      Path
*d 2001:200::/35    3FFE:1100:0:CC00::1
                               12145 10:09:15 00:57:10 1849 2914 4697 2500
* 2001:218::/35    2001:0DB8:0:F004::1
                               2      00:03:44      3462 4697
```

Table 30 describes the significant fields shown in the display.

Table 30 *show bgp ipv6 flap-statistics Field Descriptions*

| Field | Description |
|-------------------|---|
| BGP table version | Internal version number of the table. This number is incremented whenever the table changes. |
| local router ID | A 32-bit number written as 4 octets separated by periods (dotted-decimal format). |
| Status codes | Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP session. |

Table 30 *show bgp ipv6 flap-statistics Field Descriptions (continued)*

| Field | Description |
|--------------|---|
| Origin codes | Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from the Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP. |
| Network | Route to the network indicated is dampened. |
| From | IPv6 address of the peer that advertised this path. |
| Flaps | Number of times the route has flapped. |
| Duration | Time (hours:minutes:seconds) since the router noticed the first flap. |
| Reuse | Time (in hours:minutes:seconds) after which the path will be made available. |
| Path | Autonomous system path of the route that is being dampened. |

Related Commands

| Command | Description |
|---------------------------------------|---|
| bgp dampening | Enables BGP route dampening or changes various BGP route dampening factors. |
| clear bgp ipv6 flap-statistics | Clears IPv6 BGP flap statistics. |
| ip as-path access-list | Defines a BGP autonomous system path access list. |

show bgp ipv6 inconsistent-as

To display IPv6 Border Gateway Protocol (BGP) routes with inconsistent originating autonomous systems, use the **show bgp ipv6 inconsistent-as** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {unicast | multicast} inconsistent-as

| Syntax | Description |
|------------------|--|
| unicast | Specifies IPv6 unicast address prefixes. |
| multicast | Specifies IPv6 multicast address prefixes. |

| | |
|---------------|------------------------------|
| Command Modes | User EXEC Privileged EXEC |
|---------------|------------------------------|

| Command History | Release | Modification |
|-----------------|------------|---|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| | 12.3(2)T | The unicast keyword was added. |
| | 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

| | |
|------------------|--|
| Usage Guidelines | <p>The show bgp ipv6 inconsistent-as and show bgp ipv6 unicast inconsistent-as commands provide output similar to the show ip bgp inconsistent-as command, except they are IPv6-specific.</p> <p>The unicast keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the unicast keyword is mandatory starting with Cisco IOS Release 12.3(2)T.</p> <p>The multicast keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the unicast or multicast keyword is mandatory starting with Cisco IOS Release 12.0(26)S.</p> |
|------------------|--|

| | |
|----------|---|
| Examples | The following is sample output from the show bgp ipv6 inconsistent-as command: |
|----------|---|



Note

The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast inconsistent-as

BGP table version is 12612, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
```

Origin codes: i - IGP, e - EGP, ? - incomplete

| Network | Next Hop | Metric | LocPrf | Weight | Path |
|------------------|---------------------|--------|--------|---------------------|------|
| * 3FFE:1300::/24 | 2001:0DB8:0:F004::1 | | | 0 3320 293 6175 ? | |
| * | 3FFE:C00:E:9::2 | | | 0 1251 4270 10318 ? | |
| * | 3FFE:3600::A | | | 0 3462 6175 ? | |
| * | 3FFE:700:20:1::11 | | | 0 293 6175 ? | |

Table 31 describes the significant fields shown in the display.

Table 31 show bgp ipv6 inconsistent-as Field Descriptions

| Field | Description |
|-------------------|---|
| BGP table version | Internal version number of the table. This number is incremented whenever the table changes. |
| local router ID | A 32-bit number written as 4 octets separated by periods (dotted decimal format). |
| Status codes | Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP session. |
| Origin codes | Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from the Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP. |
| Network | IPv6 address of the network the entry describes. |
| Next Hop | IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network. |
| Metric | The value of the interautonomous system metric. This field is frequently not used. |
| LocPrf | Local preference value as set with the set local-preference route-map configuration command. The default value is 100. |
| Weight | Weight of the route as set via autonomous system filters. |
| Path | Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. |

show bgp ipv6 labels

To display the status of all IPv6 Border Gateway Protocol (BGP) connections, use the **show bgp ipv6 labels** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {unicast | multicast} labels

| Syntax | Description |
|------------------|--|
| unicast | Specifies IPv6 unicast address prefixes. |
| multicast | Specifies IPv6 multicast address prefixes. |

Defaults No default behavior or values

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.3(2)T | This command was introduced. |
| | 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines Use of the **unicast** keyword is mandatory with the **show bgp ipv6 labels** command.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples The following is sample output from the **show bgp ipv6 labels** command:



Note

The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast labels
```

```
Network                Next Hop           In label/Out label
2001:1:101::1/128      ::FFFF:172.17.1.1  nolabel/19
2001:3:101::1/128      ::FFFF:172.25.8.8  nolabel/19
```

Table 32 describes the significant fields shown in the display.

Table 32 *show bgp ipv6 labels Field Descriptions*

| Field | Description |
|--------------------|--|
| Network | IPv6 address of the network the entry describes. |
| Next Hop | IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network. |
| In label/Out label | IPv6 BGP connections. |

show bgp ipv6 neighbors

To display information about IPv6 Border Gateway Protocol (BGP) connections to neighbors, use the **show bgp ipv6 neighbors** command in user EXEC or privileged EXEC mode.

show bgp ipv6 { unicast | multicast } neighbors [ipv6-address] [received-routes | routes | flap-statistics | advertised-routes | paths *regular-expression* | dampened-routes]

| Syntax Description | | |
|--|--|--|
| unicast | | Specifies IPv6 unicast address prefixes. |
| multicast | | Specifies IPv6 multicast address prefixes. |
| <i>ipv6-address</i> | | (Optional) Address of the IPv6 BGP-speaking neighbor. If you omit this argument, all IPv6 neighbors are displayed. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| received-routes | | (Optional) Displays all received routes (both accepted and rejected) from the specified neighbor. |
| routes | | (Optional) Displays all routes received and accepted. This is a subset of the output from the received-routes keyword. |
| flap-statistics | | (Optional) Displays flap statistics for the routes learned from the neighbor. |
| advertised-routes | | (Optional) Displays all the routes the networking device advertised to the neighbor. |
| paths <i>regular-expression</i> | | (Optional) Regular expression used to match the paths received. |
| dampened-routes | | (Optional) Displays the dampened routes to the neighbor at the IP address specified. |

| Command Modes | User EXEC Privileged EXEC |
|---------------|------------------------------|
|---------------|------------------------------|

| Command History | Release | Modification |
|-----------------|------------|---|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | IPv6 capability information was added to the display. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| | 12.3(2)T | The unicast keyword was added. |
| | 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

| Usage Guidelines | The show bgp ipv6 neighbors and show bgp ipv6 unicast neighbors commands provide output similar to the show ip bgp neighbors command, except they are IPv6-specific. |
|------------------|---|
|------------------|---|

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples



Note

The following is sample output from the **show bgp ipv6 neighbors** command:

The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast neighbors
```

```
BGP neighbor is 3FFE:700:20:1::11, remote AS 65003, external link
Member of peer-group 6BONE for session parameters
  BGP version 4, remote router ID 192.168.2.27
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv6 Unicast: advertised and received
Received 31306 messages, 20 notifications, 0 in queue
Sent 14298 messages, 1 notifications, 0 in queue
Default minimum time between advertisement runs is 30 seconds
```

```
For address family: IPv6 Unicast
  BGP table version 21880, neighbor version 21880
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  6BONE peer-group member
  Community attribute sent to this neighbor
  Outbound path policy configured
  Incoming update prefix filter list is bgp-in
  Outgoing update prefix filter list is aggregate
  Route map for outgoing advertisements is uni-out
  77 accepted prefixes consume 4928 bytes
  Prefix advertised 4303, suppressed 0, withdrawn 1328
  Number of NLRI in the update sent: max 1, min 0
  1 history paths consume 64 bytes

  Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
  Connection state is ESTAB, I/O status: 1, unread input bytes: 0
  Local host: 3FFE:700:20:1::12, Local port: 55345
  Foreign host: 3FFE:700:20:1::11, Foreign port: 179
```

```
Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)
```

```
Event Timers (current time is 0x1A0D543C):
Timer           Starts      Wakeups      Next
Retrans         1218         5            0x0
TimeWait        0            0            0x0
AckHold         3327        3051         0x0
SendWnd         0            0            0x0
KeepAlive       0            0            0x0
```

```

GiveUp          0          0          0x0
PmtuAger        0          0          0x0
DeadWait        0          0          0x0

iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354  sndwnd: 15531
irs: 821333727  rcvnxt: 821591465  rcvwnd: 15547  delrcvwnd: 837

SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle

Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent: 4445 (retransmit: 5), with data: 4445, total data bytes: 244128

```

The following is sample output from the **show bgp ipv6 neighbors** command when the router is configured to allow IPv6 traffic to be transported across an IPv4 Multiprotocol Label Switching (MPLS) network (Cisco 6PE) without any software or hardware upgrade in the IPv4 core infrastructure. A new neighbor capability is added to show that an MPLS label is assigned for each IPv6 address prefix to be advertised. 6PE uses multiprotocol BGP to provide the reachability information for the 6PE routers across the IPv4 network so that the neighbor addresses are IPv4.

Router# **show bgp ipv6 neighbors**

```

BGP neighbor is 10.11.11.1, remote AS 65000, internal link
  BGP version 4, remote router ID 10.11.11.1
  BGP state = Established, up for 04:00:53
  Last read 00:00:02, hold time is 15, keepalive interval is 5 seconds
  Configured hold time is 15, keepalive interval is 10 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv6 Unicast: advertised and received
    ipv6 MPLS Label capability: advertised and received
  Received 67068 messages, 1 notifications, 0 in queue
  Sent 67110 messages, 16 notifications, 0 in queue
  Default minimum time between advertisement runs is 5 seconds

For address family: IPv6 Unicast
  BGP table version 91, neighbor version 91
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  Sending Prefix & Label
  4 accepted prefixes consume 288 bytes
  Prefix advertised 90, suppressed 0, withdrawn 2
  Number of NLRI in the update sent: max 3, min 0

Connections established 26; dropped 25
  Last reset 04:01:20, due to BGP Notification sent, hold time expired
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 10.10.10.1, Local port: 179
Foreign host: 10.11.11.1, Foreign port: 11003

```

Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)

```

Event Timers (current time is 0x1429F084):
Timer      Starts    Wakeups    Next
Retrans     2971         77       0x0
TimeWait         0          0       0x0
AckHold     2894       1503       0x0
SendWnd         0          0       0x0
KeepAlive         0          0       0x0
GiveUp         0          0       0x0
PmtuAger         0          0       0x0

```

```

DeadWait          0          0          0x0

iss: 803218558  snduna: 803273755  sndnxt: 803273755  sndwnd: 16289
irs: 4123967590 rcvnxt: 4124022787 rcvwnd: 16289  delrcvwnd: 95

SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 32 ms, maxRTT: 408 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs

Datagrams (max data segment is 536 bytes):
Rcvd: 4531 (out of order: 0), with data: 2895, total data bytes: 55215
Sent: 4577 (retransmit: 77, fastretransmit: 0), with data: 2894, total data
bytes: 55215

```

Table 33 describes the significant fields shown in the display.

Table 33 *show bgp ipv6 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. |
| remote AS | Autonomous system of the neighbor. |
| internal link | Indicates that this peer is an interior Border Gateway Protocol (iBGP) peer. |
| BGP version | BGP version being used to communicate with the remote router; the router ID (an IP address) of the neighbor is also specified. |
| remote router ID | A 32-bit number written as 4 octets separated by periods (dotted-decimal format). |
| BGP state | Internal state of this BGP connection. |
| up for | Amount of time that the underlying TCP connection has been in existence. |
| Last read | Time that BGP last read a message from this neighbor. |
| hold time | Maximum amount of time that can elapse between messages from the peer. |
| keepalive interval | Time period between sending keepalive packets, which help ensure that the TCP connection is up. |
| Neighbor capabilities | BGP capabilities advertised and received from this neighbor. |
| Route refresh | Indicates that the neighbor supports dynamic soft reset using the route refresh capability. |
| Address family IPv6 Unicast | Indicates that BGP peers are exchanging IPv6 reachability information. |
| ipv6 MPLS Label capability | Indicates that MPLS labels are being assigned to IPv6 address prefixes. |
| Received | Number of total BGP messages received from this peer, including keepalives. |
| notifications | Number of error messages received from the peer. |
| Sent | Total number of BGP messages that have been sent to this peer, including keepalives. |
| notifications | Number of error messages the router has sent to this peer. |
| advertisement runs | Value of the minimum advertisement interval. |
| For address family | Address family to which the following fields refer. |

Table 33 *show bgp ipv6 neighbors Field Descriptions (continued)*

| Field | Description |
|---|---|
| BGP table version | Indicates that the neighbor has been updated with this version of the primary BGP routing table. |
| neighbor version | Number used by the software to track the prefixes that have been sent and those that must be sent to this neighbor. |
| Route refresh request | Number of route refresh requests sent and received from this neighbor. |
| Community attribute (not shown in sample output) | Appears if the neighbor send-community command is configured for this neighbor. |
| Inbound path policy (not shown in sample output) | Indicates whether an inbound filter list or route map is configured. |
| Outbound path policy (not shown in sample output) | Indicates whether an outbound filter list, route map, or unsuppress map is configured. |
| bgp-in (not shown in sample output) | Name of the inbound update prefix filter list for the IPv6 unicast address family. |
| aggregate (not shown in sample output) | Name of the outbound update prefix filter list for the IPv6 unicast address family. |
| uni-out (not shown in sample output) | Name of the outbound route map for the IPv6 unicast address family. |
| accepted prefixes | Number of prefixes accepted. |
| Prefix advertised | Number of prefixes advertised. |
| suppressed | Number of prefixes suppressed. |
| withdrawn | Number of prefixes withdrawn. |
| history paths (not shown in sample output) | Number of path entries held to remember history. |
| Connections established | Number of times the router has established a TCP connection and the two peers have agreed to speak BGP with each other. |
| dropped | Number of times that a good connection has failed or been taken down. |
| Last reset | Elapsed time (in hours:minutes:seconds) since this peering session was last reset. |
| Connection state | State of the BGP peer. |
| unread input bytes | Number of bytes of packets still to be processed. |
| Local host, Local port | Peering address of the local router, plus the port. |
| Foreign host, Foreign port | Peering address of the neighbor. |
| Event Timers | Table that displays the number of starts and wakeups for each timer. |
| iss | Initial send sequence number. |
| snduna | Last send sequence number for which the local host sent but has not received an acknowledgment. |

Table 33 show bgp ipv6 neighbors Field Descriptions (continued)

| Field | Description |
|------------------|--|
| sndnxt | Sequence number the local host will send next. |
| sndwnd | TCP window size of the remote host. |
| irs | Initial receive sequence number. |
| rcvnxt | Last receive sequence number the local host has acknowledged. |
| rcvwnd | TCP window size of the local host. |
| delrecvwnd | Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field. |
| SRTT | A calculated smoothed round-trip timeout (in milliseconds). |
| RTTO | Round-trip timeout (in milliseconds). |
| RTV | Variance of the round-trip time (in milliseconds). |
| KRTT | New round-trip timeout (in milliseconds) using the Karn algorithm. This field separately tracks the round-trip time of packets that have been re-sent. |
| minRTT | Smallest recorded round-trip timeout (in milliseconds) with hard wire value used for calculation. |
| maxRTT | Largest recorded round-trip timeout (in milliseconds). |
| ACK hold | Time (in milliseconds) the local host will delay an acknowledgment in order to “piggyback” data on it. |
| Flags | IP precedence of the BGP packets. |
| Datagrams: Rcvd | Number of update packets received from neighbor. |
| with data | Number of update packets received with data. |
| total data bytes | Total number of bytes of data. |
| Sent | Number of update packets sent. |
| with data | Number of update packets with data sent. |
| total data bytes | Total number of data bytes. |

The following is sample output from the **show bgp ipv6 neighbors** command with the **advertised-routes** keyword:

```
Router# show bgp ipv6 neighbors 3FFE:700:20:1::11 advertised-routes

BGP table version is 21880, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11      0  293 3425 2500 i
*> 2001:208::/35    3FFE:C00:E:B::2        0  237 7610 i
*> 2001:218::/35    3FFE:C00:E:C::2        0  3748 4697 i
```

The following is sample output from the **show bgp ipv6 neighbors** command with the **routes** keyword:

```
Router# show bgp ipv6 neighbors 3FFE:700:20:1::11 routes
```



```

BGP table version is 21885, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

```

```

      Network          Next Hop          Metric LocPrf Weight Path
*> 2001:200::/35      3FFE:700:20:1::11              0 293 3425 2500 i
* 2001:208::/35      3FFE:700:20:1::11              0 293 7610 i
* 2001:218::/35      3FFE:700:20:1::11              0 293 3425 4697 i
* 2001:230::/35      3FFE:700:20:1::11              0 293 1275 3748 i

```

Table 34 describes the significant fields shown in the display.

Table 34 *show bgp ipv6 neighbors advertised-routes and routes Field Descriptions*

| Field | Description |
|-------------------|---|
| BGP table version | Internal version number of the table. This number is incremented whenever the table changes. |
| local router ID | A 32-bit number written as 4 octets separated by periods (dotted-decimal format). |
| Status codes | Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP session. |
| Origin codes | Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from the Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP. |
| Network | IPv6 address of the network the entry describes. |
| Next Hop | IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network. |
| Metric | The value of the interautonomous system metric. This field is frequently not used. |
| LocPrf | Local preference value as set with the set local-preference route-map configuration command. The default value is 100. |
| Weight | Weight of the route as set via autonomous system filters. |
| Path | Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. |

The following is sample output from the **show bgp ipv6 neighbors** command with the **paths** keyword:

```
Router# show bgp ipv6 neighbors 3FFE:700:20:1::11 paths ^293
```

| Address | Refcount | Metric | Path |
|------------|----------|---------------------------|------|
| 0x6131D7DC | 2 | 0 293 3425 2500 | i |
| 0x6132861C | 2 | 0 293 7610 | i |
| 0x6131AD18 | 2 | 0 293 3425 4697 | i |
| 0x61324084 | 2 | 0 293 1275 3748 | i |
| 0x61320E0C | 1 | 0 293 3425 2500 2497 | i |
| 0x61326928 | 1 | 0 293 3425 2513 | i |
| 0x61327BC0 | 2 | 0 293 | i |
| 0x61321758 | 1 | 0 293 145 | i |
| 0x61320BEC | 1 | 0 293 3425 6509 | i |
| 0x6131AAF8 | 2 | 0 293 1849 2914 | ? |
| 0x61320FE8 | 1 | 0 293 1849 1273 209 | i |
| 0x613260A8 | 2 | 0 293 1849 | i |
| 0x6132586C | 1 | 0 293 1849 5539 | i |
| 0x6131BBF8 | 2 | 0 293 1849 1103 | i |
| 0x6132344C | 1 | 0 293 4554 1103 1849 1752 | i |
| 0x61324150 | 2 | 0 293 1275 559 | i |
| 0x6131E5AC | 2 | 0 293 1849 786 | i |
| 0x613235E4 | 1 | 0 293 1849 1273 | i |
| 0x6131D028 | 1 | 0 293 4554 5539 8627 | i |
| 0x613279E4 | 1 | 0 293 1275 3748 4697 3257 | i |
| 0x61320328 | 1 | 0 293 1849 1273 790 | i |
| 0x6131EC0C | 2 | 0 293 1275 5409 | i |

**Note**

The caret (^) symbol in the example is a regular expression that is entered by simultaneously pressing the Shift and 6 keys on your keyboard. A caret (^) symbol at the beginning of a regular expression matches the start of a line.

Table 35 describes the significant fields shown in the display.

Table 35 *show bgp ipv6 neighbors paths Field Descriptions*

| Field | Description |
|----------|---|
| Address | Internal address where the path is stored. |
| Refcount | Number of routes using that path. |
| Metric | The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.) |
| Path | The autonomous system path for that route, followed by the origin code for that route. |

The following sample output from the **show bgp ipv6 neighbors** command shows the dampened routes for IPv6 address 3FFE:700:20:1::11:

```
Router# show bgp ipv6 neighbors 3FFE:700:20:1::11 dampened-routes
```

```
BGP table version is 32084, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

| Network | From | Reuse | Path |
|-------------------|-------------------|----------------------------|------|
| *d 3FFE:8030::/28 | 3FFE:700:20:1::11 | 00:24:20 293 1275 559 8933 | i |

The following sample output from the **show bgp ipv6 neighbors** command shows the flap statistics for IPv6 address 3FFE:700:20:1::11:

```
Router# show bgp ipv6 neighbors 3FFE:700:20:1::11 flap-statistics
```

```
BGP table version is 32084, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

| Network | From | Flaps | Duration | Reuse | Path |
|-------------------|-----------------|-------|----------|----------|--------------------|
| *d 2001:668::/35 | 3FFE:700:20:1:: | 4923 | 2d12h | 00:59:50 | 293 1849 3257 |
| *d 3FFE::/24 | 3FFE:700:20:1:: | 4799 | 2d12h | 00:59:30 | 293 1849 5609 4554 |
| *d 3FFE:8030::/28 | 3FFE:700:20:1:: | 95 | 11:48:24 | 00:23:20 | 293 1275 559 8933 |

The following sample output from the **show bgp ipv6 neighbors** command shows the received routes for IPv6 address 2000:0:0:4::2:

```
Router# show bgp ipv6 neighbors 2000:0:0:4::2 received-routes
```

```
BGP table version is 2443, local router ID is 192.168.0.2
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
```

| Network | Next Hop | Metric | LocPrf | Weight | Path |
|----------------------|---------------|--------|--------|--------|------|
| *> 2000:0:0:1::/64 | 2000:0:0:4::2 | | | 0 2 1 | i |
| *> 2000:0:0:2::/64 | 2000:0:0:4::2 | | | 0 2 | i |
| *> 2000:0:0:2:1::/80 | 2000:0:0:4::2 | | | 0 2 | ? |
| *> 2000:0:0:3::/64 | 2000:0:0:4::2 | | | 0 2 | ? |
| * 2000:0:0:4::1/64 | 2000:0:0:4::2 | | | 0 2 | ? |

Related Commands

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

show bgp ipv6 paths

To display all the IPv6 Border Gateway Protocol (BGP) paths in the database, use the **show bgp ipv6 paths** command in user EXEC or privileged EXEC mode.

```
show bgp ipv6 {unicast | multicast} paths regular-expression
```

| | | |
|--------------------|---------------------------|--|
| Syntax Description | unicast | Specifies IPv6 unicast address prefixes. |
| | multicast | Specifies IPv6 multicast address prefixes. |
| | <i>regular-expression</i> | Regular expression that is used to match the received paths in the database. |

| | |
|---------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| | | |
|-----------------|----------------|---|
| Command History | Release | Modification |
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| | 12.3(2)T | The unicast keyword was added. |
| | 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

| | |
|------------------|---|
| Usage Guidelines | The show bgp ipv6 paths and show bgp ipv6 unicast paths commands provide output similar to the show ip bgp paths command, except they are IPv6-specific. |
| | The unicast keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the unicast keyword is mandatory starting with Cisco IOS Release 12.3(2)T. |
| | The multicast keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the unicast or multicast keyword is mandatory starting with Cisco IOS Release 12.0(26)S. |

| | |
|----------|---|
| Examples | The following is sample output from the show bgp ipv6 paths command: |
|----------|---|

**Note**

The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast paths
```

```
Address      Hash Refcount Metric Path
0x61322A78   0      2      0 i
0x6131C214   3      2      0 6346 8664 786 i
0x6131D600   13     1      0 3748 1275 8319 1273 209 i
0x613229F0   17     1      0 3748 1275 8319 12853 i
0x61324AE0   18     1      1 4554 3748 4697 5408 i
0x61326818   32     1      1 4554 5609 i
0x61324728   34     1      0 6346 8664 9009 ?
0x61323804   35     1      0 3748 1275 8319 i
0x61327918   35     1      0 237 2839 8664 ?
0x61320504   38     2      0 3748 4697 1752 i
0x61320988   41     2      0 1849 786 i
0x6132245C   46     1      0 6346 8664 4927 i
```

Table 36 describes the significant fields shown in the display.

Table 36 *show bgp ipv6 paths Field Descriptions*

| Field | Description |
|----------|---|
| Address | Internal address where the path is stored. |
| Hash | Hash bucket where the path is stored. |
| Refcount | Number of routes using that path. |
| Metric | The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.) |
| Path | The autonomous system path for that route, followed by the origin code for that route. |

show bgp ipv6 peer-group

To display information about Border Gateway Protocol (BGP) peer groups, use the **show bgp ipv6 peer-group** command in user EXEC or privileged EXEC mode.

```
show bgp ipv6 {unicast | multicast} peer-group [name]
```

| | | |
|--------------------|------------------|--|
| Syntax Description | unicast | Specifies IPv6 unicast address prefixes. |
| | multicast | Specifies IPv6 multicast address prefixes. |
| | <i>name</i> | Peer group name. |

| | |
|---------------|------------------------------|
| Command Modes | User EXEC Privileged EXEC |
|---------------|------------------------------|

| | | |
|-----------------|----------------|---|
| Command History | Release | Modification |
| | 12.3(2)T | This command was introduced. |
| | 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines

If a user does not specify a peer group name, then all BGP peer groups will be displayed.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 peer-group** command:

```
Router# show bgp ipv6 unicast peer-group

BGP peer-group is external-peerings, remote AS 20
  BGP version 4
  Default minimum time between advertisement runs is 30 seconds

For address family:IPv6 Unicast
  BGP neighbor is external-peerings, peer-group external, members:
  1::1
  Index 0, Offset 0, Mask 0x0
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent:max 0, min 0
```

Table 37 describes the significant fields shown in the display.

Table 37 *show bgp ipv6 peer-group Field Descriptions*

| Field | Description |
|-------------------------------------|---|
| BGP peer-group is | Type of BGP peer group. |
| remote AS | Autonomous system of the peer group. |
| BGP version | BGP version being used to communicate with the remote router. |
| For address family: IPv4 Unicast | IPv6 unicast-specific properties of this neighbor. |

show bgp ipv6 prefix-list

To display routes that match a prefix list, use the **show bgp ipv6 prefix-list** command in user EXEC or privileged EXEC mode.

```
show bgp ipv6 { unicast | multicast } prefix-list name
```

| | | |
|--------------------|------------------|--|
| Syntax Description | unicast | Specifies IPv6 unicast address prefixes. |
| | multicast | Specifies IPv6 multicast address prefixes. |
| | <i>name</i> | The specified prefix list. |

| | |
|---------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| | | |
|-----------------|----------------|---|
| Command History | Release | Modification |
| | 12.3(2)T | This command was introduced. |
| | 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines

The specified prefix list must be an IPv6 prefix list, which is similar in format to an IPv4 prefix list.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 prefix-list** command:

```
Router# show ipv6 prefix-list unicast detail

ipv6 prefix-list pin:
  count:4, range entries:3, sequences:5 - 20, refcount:2
  seq 5 permit 747::/16 (hit count:1, refcount:2)
  seq 10 permit 747:1::/32 ge 64 le 64 (hit count:2, refcount:2)
  seq 15 permit 747::/32 ge 33 (hit count:1, refcount:1)
  seq 20 permit 777::/16 le 124 (hit count:2, refcount:1)

The ipv6 prefix-list match the following prefixes:

  seq 5: matches the exact match 747::/16
  seq 10: first 32 bits in prefix must match with a prefixlen of /64
  seq 15: first 32 bits in prefix must match with any prefixlen up to /128
  seq 20: first 16 bits in prefix must match with any prefixlen up to /124
```

Table 38 describes the significant fields shown in the display.

Table 38 *show bgp ipv6 prefix-list Field Descriptions*

| Field | Description |
|-------------------|---|
| BGP table version | Internal version number of the table. This number is incremented whenever the table changes. |
| local router ID | A 32-bit number written as 4 octets separated by periods (dotted-decimal format). |
| Status codes | Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP session. |
| Origin codes | Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from the Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP. |
| Network | IPv6 address of the network the entry describes. |
| Next Hop | IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network. |
| Metric | The value of the interautonomous system metric. This field is frequently not used. |
| LocPrf | Local preference value as set with the set local-preference route-map configuration command. The default value is 100. |
| Weight | Weight of the route as set via autonomous system filters. |
| Path | Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. |

show bgp ipv6 quote-regexp

To display IPv6 Border Gateway Protocol (BGP) routes matching the autonomous system path regular expression as a quoted string of characters, use the **show bgp ipv6 quote-regexp** command in user EXEC or privileged EXEC mode.

```
show bgp ipv6 {unicast | multicast} quote-regexp regular-expression
```

| | | |
|--------------------|---------------------------|---|
| Syntax Description | unicast | Specifies IPv6 unicast address prefixes. |
| | multicast | Specifies IPv6 multicast address prefixes. |
| | <i>regular-expression</i> | Regular expression that is used to match the BGP autonomous system paths. |

| | |
|---------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| Command History | Release | Modification |
|-----------------|------------|---|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| | 12.3(2)T | The unicast keyword was added. |
| | 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines The **show bgp ipv6 quote-regexp** and **show bgp ipv6 unicast quote-regexp** commands provide output similar to the **show ip bgp quote-regexp** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples The following is sample output from the **show bgp ipv6 quote-regexp** command that shows paths beginning with 33 or containing 293:

**Note**

The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast quote-regexp ^33|293
```

```
BGP table version is 69964, local router ID is 192.31.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2      1           0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1
                                0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2      1           0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2      0 6389 1849 293 2713 i
*  3FFE::/24        3FFE:C00:E:5::2      0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2      0 33 1849 3263 i
*  3FFE:300::/24    3FFE:C00:E:5::2      0 33 293 1275 1717 i
*                   3FFE:C00:E:F::2      0 6389 1849 293 1275
```

**Note**

The caret (^) symbol in the example is a regular expression that is entered by pressing the Shift and 6 keys on your keyboard. A caret (^) symbol at the beginning of a regular expression matches the start of a line.

Table 39 describes the significant fields shown in the display.

Table 39 *show bgp ipv6 quote-regexp Field Descriptions*

| Field | Description |
|-------------------|---|
| BGP table version | Internal version number of the table. This number is incremented whenever the table changes. |
| local router ID | A 32-bit number written as 4 octets separated by periods (dotted-decimal format). |
| Status codes | Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP session. |

Table 39 *show bgp ipv6 quote-regexp Field Descriptions (continued)*

| Field | Description |
|--------------|---|
| Origin codes | Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from the Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP. |
| Network | IPv6 address of the network the entry describes. |
| Next Hop | IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network. |
| Metric | The value of the interautonomous system metric. This field is frequently not used. |
| LocPrf | Local preference value as set with the set local-preference route-map configuration command. The default value is 100. |
| Weight | Weight of the route as set via autonomous system filters. |
| Path | Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. |

Related Commands

| Command | Description |
|-----------------------------|--|
| show bgp ipv6 regexp | Displays IPv6 BGP routes matching the autonomous system path regular expression. |
| show ip bgp regexp | Displays routes matching the regular expression. |

show bgp ipv6 regexp

To display IPv6 Border Gateway Protocol (BGP) routes matching the autonomous system path regular expression, use the **show bgp ipv6 regexp** command in user EXEC or privileged EXEC mode.

show bgp ipv6 { unicast | multicast } regexp *regular-expression*

| | | |
|--------------------|---------------------------|---|
| Syntax Description | unicast | Specifies IPv6 unicast address prefixes. |
| | multicast | Specifies IPv6 multicast address prefixes. |
| | <i>regular-expression</i> | Regular expression that is used to match the BGP autonomous system paths. |

| | |
|----------|-------------------------------|
| Defaults | No default behavior or values |
|----------|-------------------------------|

| | |
|---------------|------------------------------|
| Command Modes | User EXEC Privileged EXEC |
|---------------|------------------------------|

| Command History | Release | Modification |
|-----------------|------------|---|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| | 12.3(2)T | The unicast keyword was added. |
| | 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

| | |
|------------------|---|
| Usage Guidelines | <p>The show bgp ipv6 regexp and show bgp ipv6 regexp commands provide output similar to the show ip bgp regexp command, except they are IPv6-specific.</p> <p>The unicast keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the unicast keyword is mandatory starting with Cisco IOS Release 12.3(2)T.</p> <p>The multicast keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the unicast or multicast keyword is mandatory starting with Cisco IOS Release 12.0(26)S.</p> |
|------------------|---|

| | |
|----------|---|
| Examples | The following is sample output from the show bgp ipv6 regexp command that shows paths beginning with 33 or containing 293: |
|----------|---|

**Note**

The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast regexp ^33|293
```

```
BGP table version is 69964, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

| | Network | Next Hop | Metric | LocPrf | Weight | Path |
|---|---------------|---------------------|--------|--------|--------|----------------------|
| * | 2001:200::/35 | 3FFE:C00:E:4::2 | 1 | | 0 | 4554 293 3425 2500 i |
| * | | 2001:0DB8:0:F004::1 | | | | |
| | | | | | 0 | 3320 293 3425 2500 i |
| * | 2001:208::/35 | 3FFE:C00:E:4::2 | 1 | | 0 | 4554 293 7610 i |
| * | 2001:228::/35 | 3FFE:C00:E:F::2 | | | 0 | 6389 1849 293 2713 i |
| * | 3FFE::/24 | 3FFE:C00:E:5::2 | | | 0 | 33 1849 4554 i |
| * | 3FFE:100::/24 | 3FFE:C00:E:5::2 | | | 0 | 33 1849 3263 i |
| * | 3FFE:300::/24 | 3FFE:C00:E:5::2 | | | 0 | 33 293 1275 1717 i |
| * | | 3FFE:C00:E:F::2 | | | 0 | 6389 1849 293 1275 |

**Note**

The caret (^) symbol in the example is a regular expression that is entered by pressing the Shift and 6 keys on your keyboard. A caret (^) symbol at the beginning of a regular expression matches the start of a line.

Table 40 describes the significant fields shown in the display.

Table 40 show bgp ipv6 regexp Field Descriptions

| Field | Description |
|-------------------|---|
| BGP table version | Internal version number of the table. This number is incremented whenever the table changes. |
| local router ID | A 32-bit number written as 4 octets separated by periods (dotted-decimal format). |
| Status codes | <p>Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values:</p> <p>s—The table entry is suppressed.</p> <p>d—The table entry is dampened.</p> <p>h—The table entry is history.</p> <p>*—The table entry is valid.</p> <p>>—The table entry is the best entry to use for that network.</p> <p>i—The table entry was learned via an internal BGP session.</p> |

Table 40 *show bgp ipv6 regexp Field Descriptions (continued)*

| Field | Description |
|--------------|---|
| Origin codes | Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from the Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP. |
| Network | IPv6 address of the network the entry describes. |
| Next Hop | IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network. |
| Metric | The value of the interautonomous system metric. This field is frequently not used. |
| LocPrf | Local preference value as set with the set local-preference route-map configuration command. The default value is 100. |
| Weight | Weight of the route as set via autonomous system filters. |
| Path | Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. |

show bgp ipv6 route-map

To display IPv6 Border Gateway Protocol (BGP) routes that failed to install in the routing table, use the **show bgp ipv6 route-map** command in user EXEC or privileged EXEC mode.

```
show bgp ipv6 {unicast | multicast} route-map name
```

| | | | |
|--------|-------------|------------------|--|
| Syntax | Description | unicast | Specifies IPv6 unicast address prefixes. |
| | | multicast | Specifies IPv6 multicast address prefixes. |
| | | <i>name</i> | A specified route map to match. |

Defaults No default behavior or values

Command Modes User EXEC
Privileged EXEC

| | | |
|-----------------|----------------|---|
| Command History | Release | Modification |
| | 12.3(2)T | This command was introduced. |
| | 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples The following is sample output from the **show bgp ipv6 route-map** command for a route map named rmap:

```
Router# show bgp ipv6 unicast route-map rmap

BGP table version is 16, local router ID is 172.30.242.1
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
*>i12:12::/64      2001:0DB8:101::1             0   100    50 ?
*>i12:13::/64      2001:0DB8:101::1             0   100    50 ?
*>i12:14::/64      2001:0DB8:101::1             0   100    50 ?
*>i543::/64        2001:0DB8:101::1             0   100    50 ?
```

Table 41 describes the significant fields shown in the display.

Table 41 *show bgp ipv6 route-map Field Descriptions*

| Field | Description |
|-------------------|--|
| BGP table version | Internal version number of the table. This number is incremented whenever the table changes. |
| local router ID | A 32-bit number written as 4 octets separated by periods (dotted-decimal format). |
| Status codes | <p>Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values:</p> <p>s—The table entry is suppressed.</p> <p>d—The table entry is dampened.</p> <p>h—The table entry is history.</p> <p>*—The table entry is valid.</p> <p>>—The table entry is the best entry to use for that network.</p> <p>i—The table entry was learned via an internal BGP session.</p> <p>r —A RIB failure has occurred.</p> <p>S—The route map is stale.</p> |
| Origin codes | <p>Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values:</p> <p>i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a network router configuration command.</p> <p>e—Entry originated from the Exterior Gateway Protocol (EGP).</p> <p>?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.</p> |
| Network | IPv6 address of the network the entry describes. |
| Next Hop | IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network. |
| Metric | The value of the interautonomous system metric. This field is frequently not used. |
| LocPrf | Local preference value as set with the set local-preference route-map configuration command. The default value is 100. |
| Weight | Weight of the route as set via autonomous system filters. |
| Path | Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. |

show bgp ipv6 summary

To display the status of all IPv6 Border Gateway Protocol (BGP) connections, use the **show bgp ipv6 summary** command in user EXEC or privileged EXEC mode.

```
show bgp ipv6 {unicast | multicast} summary
```

| | | | |
|--------|-------------|------------------|--|
| Syntax | Description | unicast | Specifies IPv6 unicast address prefixes. |
| | | multicast | Specifies IPv6 multicast address prefixes. |

Defaults No default behavior or values

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------|---|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| | 12.3(2)T | The unicast keyword was added. |
| | 12.0(26)S | The unicast and multicast keywords were added to Cisco IOS Release 12.0(26)S. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines The **show bgp ipv6 summary** and **show bgp ipv6 summary** commands provide output similar to the **show ip bgp summary** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples The following is sample output from the **show bgp ipv6 summary** command:

**Note**

The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast summary
```

```
BGP router identifier 172.30.4.4, local AS number 200
BGP table version is 1, main routing table version 1
```

| Neighbor | V | AS | MsgRcvd | MsgSent | TblVer | InQ | OutQ | Up/Down | State/PfxRcd |
|------------------|---|-----|---------|---------|--------|-----|------|----------|--------------|
| 2001:0DB8:101::2 | 4 | 200 | 6869 | 6882 | 0 | 0 | 0 | 06:25:24 | Active |

Table 42 describes the significant fields shown in the display.

Table 42 *show bgp ipv6 summary Field Descriptions*

| Field | Description |
|----------------------------|--|
| BGP router identifier | IP address of the networking device. |
| BGP table version | Internal version number of the BGP database. |
| main routing table version | Last version of BGP database that was injected into the main routing table. |
| Neighbor | IPv6 address of a neighbor. |
| V | BGP version number spoken to that neighbor. |
| AS | Autonomous system. |
| MsgRcvd | BGP messages received from that neighbor. |
| MsgSent | BGP messages sent to that neighbor. |
| TblVer | Last version of the BGP database that was sent to that neighbor. |
| InQ | Number of messages from that neighbor waiting to be processed. |
| OutQ | Number of messages waiting to be sent to that neighbor. |
| Up/Down | The length of time that the BGP session has been in state Established, or the current state if it is not Established. |
| State/PfxRcd | Current state of the BGP session/the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the neighbor maximum-prefix command) is reached, the string “PfxRcd” appears in the entry, the neighbor is shut down, and the connection is Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command. |

Related Commands

| Command | Description |
|--------------------------------|---|
| clear bgp ipv6 | Resets an IPv6 BGP TCP connection using BGP soft reconfiguration. |
| neighbor maximum-prefix | Controls how many prefixes can be received from a neighbor. |
| neighbor shutdown | Disables a neighbor or peer group. |

show cdp entry

To display information about a specific neighboring device discovered using Cisco Discovery Protocol (CDP), use the **show cdp entry** command in privileged EXEC mode.

```
show cdp entry { * | device-name[*] } [version] [protocol]
```

Syntax Description

| | |
|-----------------------|---|
| * | Displays all of the CDP neighbors. |
| device-name[*] | Name of the neighbor about which you want information. You can enter an optional asterisk (*) at the end of an <i>entry-name</i> as a wildcard. For example, entering show cdp entry dev* will match all entries which begin with dev . |
| version | (Optional) Limits the display to information about the version of software running on the router. |
| protocol | (Optional) Limits the display to information about the protocols enabled on a router. |

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|---------------------|--|
| 10.3 | This command was introduced. |
| 12.2(8)T, 12.2(14)S | Support for IPv6 address and address type information was added. |

Examples

The following is sample output from the **show cdp entry** command. Information about the neighbor *device.cisco.com* is displayed, including device ID, protocols and addresses, platform, interface, hold time, and version.

```
Router# show cdp entry device.cisco.com

-----
Device ID: device.cisco.com
Entry address(es):
  IP address: 10.1.17.24
  IPv6 address: FE80::203:E3FF:FE6A:BF81 (link-local)
  IPv6 address: 4000::BC:0:0:C0A8:BC06 (global unicast)
  CLNS address: 490001.1111.1111.1111.00
Platform: cisco 3640, Capabilities: Router
Interface: Ethernet0/1, Port ID (outgoing port): Ethernet0/1
Holdtime : 160 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-A2IS-M), Experimental Version 12.2
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 08-Aug-01 12:39 by joeuser
```

The following is sample output from the **show cdp entry version** command. Only information about the version of software running on *device.cisco.com* is displayed.

```
Router# show cdp entry device.cisco.com version
```

```

Version information for device.cisco.com:
  Cisco Internetwork Operating System Software
  IOS (tm) 3600 Software (C3640-A2IS-M), Experimental Version 12.2
  Copyright (c) 1986-2001 by cisco Systems, Inc.
  Compiled Wed 08-Aug-01 12:39 by joeuser

```

The following is sample output from the **show cdp entry protocol** command. Only information about the protocols enabled on *device.cisco.com* is displayed.

```
Router# show cdp entry device.cisco.com protocol
```

```

Protocol information for device.cisco.com:
  IP address: 10.1.17.24
  IPv6 address: FE80::203:E3FF:FE6A:BF81 (link-local)
  IPv6 address: 4000::BC:0:0:C0A8:BC06 (global unicast)
  CLNS address: 490001.1111.1111.1111.00

```

Related Commands

| Command | Description |
|---------------------------|---|
| show cdp | Displays global CDP information, including timer and hold-time information. |
| show cdp interface | Displays information about the interfaces on which CDP is enabled. |
| show cdp neighbors | Displays detailed information about neighboring devices discovered using CDP. |
| show cdp traffic | Displays traffic information from the CDP table. |

show cdp neighbors

To display detailed information about neighboring devices discovered using Cisco Discovery Protocol (CDP), use the **show cdp neighbors** command in privileged EXEC mode.

```
show cdp neighbors [type number] [detail]
```

| | | |
|--------------------|--------|---|
| Syntax Description | type | (Optional) Type of the interface connected to the neighbors about which you want information. |
| | number | (Optional) Number of the interface connected to the neighbors about which you want information. |
| | detail | (Optional) Displays detailed information about a neighbor (or neighbors) including network address, enabled protocols, hold time, and software version. |

| | |
|---------------|-----------------|
| Command Modes | Privileged EXEC |
|---------------|-----------------|

| Command History | Release | Modification |
|-----------------|---------------------|--|
| | 10.3 | This command was introduced. |
| | 12.0(3)T | The output for the detail form of this command was expanded to include CDP Version 2 information. |
| | 12.2(8)T, 12.2(14)S | Support for IPv6 address and address type information was added. |

Examples The following example specifies information related to the **show cdp neighbors** command:

```
Router# show cdp neighbors

Capability Codes:R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch,
H - Host, I - IGMP, r - Repeater
Device ID    Local Intrfce  Holdtme  Capability  Platform  Port ID
joe          Eth 0           133      R           4500      Eth 0
sam          Eth 0           152      R           AS5200    Eth 0
terri        Eth 0           144      R           3640      Eth0/0
maine        Eth 0           141      R           RP1       Eth 0/0
sancho       Eth 0           164      R           7206      Eth 1/0
```

Table 43 describes the significant fields shown in the example.

Table 43 show cdp neighbors Field Descriptions

| Field | Definition |
|------------------|---|
| Capability Codes | The type of device that can be discovered. |
| Device ID | The name of the neighbor device and either the MAC address or the serial number of this device. |
| Local Intrfce | The local interface through which this neighbor is connected. |

Table 43 *show cdp neighbors Field Descriptions*

| Field | Definition |
|------------|---|
| Holdtime | The remaining amount of time (in seconds) the current device will hold the CDP advertisement from a sending router before discarding it. |
| Capability | The type of the device listed in the CDP Neighbors table. Possible values are as follows: R—Router T—Transparent bridge B—Source-routing bridge S—Switch H—Host I—IGMP device r—Repeater |
| Platform | The product number of the device. |
| Port ID | The interface and port number of the neighboring device. |

The following is sample output for one neighbor from the **show cdp neighbors detail** command. Additional detail is shown about neighbors, including network addresses, enabled protocols, and software version.

```
router# show cdp neighbors detail
```

```
Device ID: device.cisco.com
Entry address(es):
  IPv6 address: FE80::203:E3FF:FE6A:BF81 (link-local)
  IPv6 address: 4000::BC:0:0:C0A8:BC06 (global unicast)
Platform: cisco 3640, Capabilities: Router
Interface: Ethernet0/1, Port ID (outgoing port): Ethernet0/1
Holdtime : 160 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-A2IS-M), Experimental Version 12.2
Duplex Mode: half
Native VLAN: 42
VTP Management Domain: 'Accounting Group'
```

Table 44 describes the significant fields shown in the display.

Table 44 *show cdp neighbors detail Field Descriptions*

| Field | Definition |
|-------------------|---|
| Device ID | The name of the neighbor device and either the MAC address or the serial number of this device. |
| Entry address(es) | A list of network addresses of neighbor devices. |

Table 44 *show cdp neighbors detail Field Descriptions (continued)*

| Field | Definition |
|---|---|
| IPv6 address: FE80::203:E3FF:FE6A:BF81 (link-local) | <p>The network address of the neighbor device. The address can be in IP, IPv6, IPX, AppleTalk, DECnet, or Connectionless Network Service (CLNS) protocol conventions.</p> <p>IPv6 addresses are followed by one of the following IPv6 address types:</p> <ul style="list-style-type: none"> • global unicast • link-local • multicast • site-local • V4 compatible |
| Platform | The product name and number of the neighbor device. |
| Capabilities | The device type of the neighbor. This device can be a router, a bridge, a transparent bridge, a source-routing bridge, a switch, a host, an IGMP device, or a repeater. |
| Interface | The local interface through which this neighbor is connected. |
| Port ID | The interface and port number of the neighboring device. |
| Holdtime | The remaining amount of time (in seconds) the current device will hold the CDP advertisement from a sending router before discarding it. |
| Version | The software version of the neighbor device. |
| Duplex Mode | The duplex state of connection between the current device and the neighbor device. |
| Native VLAN | The ID number of the VLAN on the neighbor device. |
| VTP Management Domain | A string that is the name of the collective group of VLANs associated with the neighbor device. |

Related Commands

| Command | Description |
|---------------------------|--|
| show cdp | Displays global CDP information, including timer and hold-time information. |
| show cdp entry | Displays information about a specific neighbor device listed in the CDP table. |
| show cdp interface | Displays information about the interfaces on which CDP is enabled. |
| show cdp traffic | Displays information about traffic between devices gathered using CDP. |

show cef

To display which packets the line cards dropped or to display which packets were not express-forwarded, use the **show cef** command in user EXEC or privileged EXEC mode.

show cef {drop | not-cef-switched}

| | | |
|---------------------------|-------------------------|--|
| Syntax Description | drop | (Optional) Displays which packets were dropped by each line card. |
| | not-cef-switched | (Optional) Displays which packets were sent to a different switching path. |

| | |
|----------------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| | | |
|------------------------|---------------------------------|--|
| Command History | Release | Modification |
| | 11.2 GS | This command was introduced to support the Cisco 12012 Internet router. |
| | 11.1 CC | Multiple platform support was added. |
| | 12.0(22)S, 12.2(13)T, 12.2(14)S | The display output for this command was modified to include support for Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEF for IPv6 (dCEFv6) packets. |

| | |
|-------------------------|---|
| Usage Guidelines | A line card might drop packets because of encapsulation failure, absence of route information, or absence of adjacency information. |
| | A packet is sent to a different switching path (punted) because CEF does not support the encapsulation or feature, the packet is destined for the router, or the packet has IP options, such as time stamp and record route. IP options are process-switched. |



Note

If CEFv6 or dCEFv6 is enabled globally on the router, the **drop** and **not-cef-switched** keywords used with the **show cef** command display IPv6 CEF counter information and IPv4 CEF counter information. If CEFv6 or dCEFv6 is not enabled globally on the router, the **drop** and **not-cef-switched** keywords used with the **show cef** command display only IPv4 CEF counter information.

| | |
|-----------------|---|
| Examples | The following is sample output from the show cef drop command: |
|-----------------|---|

```
Router# show cef drop
```

```
CEF Drop Statistics
Slot  Encap_fail  Unresolved  Unsupported  No_route  No_adj  ChksumErr
RP           4           89           0           4           0           0
1           0           0           0           0           0           0
2           0           0           5           0           0           5
IPv6 CEF Drop Statistics
Slot  Encap_fail  Unresolved  Unsupported  No_route  No_adj
RP           2           33           0           2           0
```

```

1           0           0           3           0           0
2           0           0           0           0           0

```

Table 45 describes the significant fields shown in the display.

Table 45 *show cef drop Field Descriptions*

| Field | Description |
|-------------|--|
| Slot | The slot number on which the packets were received. |
| Encap_fail | Indicates the number of packets dropped after exceeding the limit for packets punted to the processor due to missing adjacency information. (CEF throttles packets passed up to the process level at a rate of one packet per second.) |
| Unresolved | Indicates the number of packets dropped due to an unresolved prefix in the Forwarding Information Base (FIB) table. |
| Unsupported | Indicates the number of packets fast-dropped by CEF (drop adjacency). |
| No_route | Indicates the number of packets dropped due to a missing prefix in the FIB table. |
| No_adj | Indicates the number of packets dropped due to incomplete adjacency. |
| ChksumErr | Indicates the number of IPv4 packets received with a checksum error. Note This field is not supported for IPv6 packets. |

The following is sample output from the **show cef not-cef-switched** command:

Router# **show cef not-cef-switched**

```

CEF Packets passed on to next switching layer
Slot No_adj No_encap Unsupp'ted Redirect Receive Options Access Frag
RP      0      0      0      0      91584      0      0      0
1       0      0      0      0      0        0      0      0
2       0      0      0      0      0        0      0      0
IPv6 CEF Packets passed on to next switching layer
Slot No_adj No_encap Unsupp'ted Redirect Receive Options Access MTU
RP      0      0      0      0      92784      0      0      0
1       0      0      0      0      0        0      0      0
2       0      0      0      0      0        0      0      0

```

Table 46 describes the significant fields shown in the display.

Table 46 *show cef not-cef-switched Field Descriptions*

| Field | Meaning |
|------------|---|
| No_adj | Indicates the number of packets sent to the processor due to incomplete adjacency. |
| No_encap | Indicates the number of packets sent to the processor for Address Resolution Protocol (ARP) resolution. |
| Unsupp'ted | Indicates the number of packets punted to the next switching level due to unsupported features. |

Table 46 *show cef not-cef-switched Field Descriptions (continued)*

| Field | Meaning |
|----------|--|
| Redirect | Records packets that are ultimately destined to the router, and packets destined to a tunnel endpoint on the router. If the decapsulated tunnel is IP, it is CEF-switched; otherwise packets are process-switched. |
| Receive | Indicates the number of packets ultimately destined to the router, or packets destined to a tunnel endpoint on the router. If the decapsulated tunnel packet is IP, the packet is CEF-switched. Otherwise, packets are process-switched. |
| Options | Indicates the number of packets with options. Packets with IP options are handled only at the process level. |
| Access | Indicates the number of packets punted due to an access list failure. |
| Frag | Indicates the number of packets punted due to fragmentation failure. Note This field is not supported for IPv6 packets. |
| MTU | Indicates the number of packets punted due to maximum transmission unit (MTU) failure. Note This field is not supported for IPv4 packets. |

Related Commands

| Command | Description |
|---------------------------|--|
| show cef interface | Displays CEF-related interface information. |
| show cef linecard | Displays CEF-related interface information by line card. |

show cef interface

To display detailed Cisco Express Forwarding (CEF) information for all interfaces, use the **show cef interface** command in user EXEC or privileged EXEC mode.

```
show cef interface [type number] [statistics] [detail]
```

| | | |
|--------------------|--------------------|---|
| Syntax Description | <i>type number</i> | (Optional) Interface type and number. |
| | statistics | (Optional) Displays switching statistics for the line card. |
| | detail | (Optional) Displays detailed CEF information for the specified interface type and number. |

| | |
|---------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| | | |
|-----------------|----------------------|--|
| Command History | Release | Modification |
| | 11.2 GS | This command was introduced to support the Cisco 12012 Internet router. |
| | 11.1 CC | Multiple platform support was added. |
| | 12.0(14)ST | Documentation for the statistics keyword was updated. |
| | 12.2(2)T | Documentation for the statistics and detail keywords was updated. |
| | 12.0(22)S, 12.2(14)S | The display output for this command was modified to include support for CEF for IPv6 (CEFv6) and distributed (dCEFv6) interface information. |

Usage Guidelines

You can use this command to display the detailed CEF status for all of the interfaces.

Values entered for the *type* and *number* arguments display CEF status information for the specified interface type and number.

Examples

The following is sample output from the **show cef interface detail** command for Ethernet interface 1/0/0:

```
Router# show cef interface Ethernet 1/0/0 detail

Ethernet1/0/0 is up (if_number 9)
  Corresponding hwidb fast_if_number 9
  Corresponding hwidb firstsw->if_number 9
  Internet address is 10.2.61.8/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  Hardware idb is Ethernet1/0/0
  Fast switching type 1, interface type 5
  IP Distributed CEF switching enabled
  IP Feature Fast switching turbo vector
```

```

IP Feature CEF switching turbo vector
Input fast flags 0x0, Output fast flags 0x0
ifindex 7(7)
Slot 1 Slot unit 0 VC -1
Transmit limit accumulator 0x48001A82 (0x48001A82)
IP MTU 1500

```

The following is sample output from the **show cef interface Null 0 detail** command:

```
Router# show cef interface Null 0 detail
```

```

Null0 is up (if_number 1)
  Corresponding hwidb fast_if_number 1
  Corresponding hwidb firstsw->if_number 1
  Internet Protocol processing disabled
  Interface is marked as nullidb
  Packets switched to this interface on linecard are dropped to next slow path
  Hardware idb is Null0
  Fast switching type 13, interface type 0
  IP CEF switching enabled
  IP Feature CEF switching turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 0(0)
  Slot -1 Slot unit -1 VC -1
  Transmit limit accumulator 0x0 (0x0)
  IP MTU 1500

```

Table 47 describes the significant fields shown in the displays.

Table 47 *show cef interface Field Descriptions*

| Field | Description |
|--|--|
| Ethernet1/0/0 is up | Indicates type, number, and status of the interface. |
| Internet address is | Internet address of the interface. |
| ICMP redirects are always sent | Indicates how packet forwarding is configured. |
| Per packet load-sharing is disabled | Indicates status of load sharing on the interface. |
| IP unicast RPF check is disabled | Indicates status of IP unicast Reverse Path Forwarding (RPF) check on the interface. |
| Inbound access list is not set | Indicates the number or name of the inbound access list if one is applied to this interface. |
| Outbound access list is not set | Indicates the number or name of the outbound access list if one is applied to this interface. |
| IP policy routing is disabled | Indicates the status of IP policy routing on the interface. |
| Hardware idb is Ethernet1/0/0 | Interface type and number configured. |
| Fast switching type | Used for troubleshooting; indicates switching mode in use. |
| interface type 5 | Indicates interface type. |
| IP Distributed CEF switching enabled | Indicates whether distributed CEF is enabled on this interface. (Cisco 7500 and 12000 series Internet routers only.) |
| IP Feature Fast switching turbo vector | Indicates IP fast switching type configured. |

Table 47 *show cef interface Field Descriptions (continued)*

| Field | Description |
|---------------------------------------|---|
| IP Feature CEF switching turbo vector | Indicates IP feature CEF switching type configured. |
| Input fast flags | <p>Indicates the input status of various switching features, as follows:</p> <ul style="list-style-type: none"> • 0x0001 (input Access Control List [ACL] enabled) • 0x0002 (policy routing enabled) • 0x0004 (input rate limiting) • 0x0008 (MAC/Prec accounting) • 0x0010 (DSCP/PREC/QOS GROUP) • 0x0020 (input named access lists) • 0x0040 (NAT enabled on input) • 0x0080 (crypto map on input) • 0x0100 (QPPB classification) • 0x0200 (inspect on input) • 0x0400 (input classification) • 0x0800 (casa input enable) • 0x1000 (Virtual Private Network [VPN] enabled on a swidb) • 0x2000 (input idle timer enabled) • 0x4000 (unicast Reverse Path Forwarding [RPF] check) • 0x8000 (per-address ACL enabled) • 0x10000 (Deaggregating a packet) • 0x20000 (GPRS enabled on input) • 0x40000 (URL RenDezvous) • 0x80000 (QoS classification) • 0x100000 (FR switching on i/f) • 0x200000 (WCCP redirect on input) • 0x400000 (input classification) |

Table 47 *show cef interface Field Descriptions (continued)*

| Field | Description |
|----------------------------|---|
| Output fast flags | <p>Indicates the output status of various switching features, as follows:</p> <ul style="list-style-type: none"> • 0x0001 (output ACL enabled) • 0x0002 (IP accounting enabled) • 0x0004 (WCC redirect enable i/f) • 0x0008 (rate limiting) • 0x0010 (MAC/Prec accounting) • 0x0020 (DSCP/PREC/QOS GROUP) • 0x0040 (D-QOS classification) • 0x0080 (output named access lists) • 0x0100 (NAT enabled on output) • 0x0200 (TCP intercept enabled) • 0x0400 (crypto map set on output) • 0x0800 (output firewall) • 0x1000 (RSVP classification) • 0x2000 (inspect on output) • 0x4000 (QoS classification) • 0x8000 (QoS pre-classification) • 0x10000 (output stile) |
| ifindex 7/(7) | Indicates the SNMP ifindex for this interface. |
| Slot 1 Slot unit 0 VC -1 | The slot number and slot unit. |
| Transmit limit accumulator | Indicates the maximum number of packets allowed in the transmit queue. |
| IP MTU | The MTU size set on the interface. |

Related Commands

| Command | Description |
|--------------------------|---|
| show cef | Displays which packets the line cards dropped or displays which packets were not express-forwarded. |
| show cef linecard | Displays CEF-related interface information by line card. |

show cef linecard

To display Cisco Express Forwarding (CEF)-related information by line card, use the **show cef linecard** command in user EXEC or privileged EXEC mode.

show cef linecard [*slot-number*] [**detail**] [**internal**]

Syntax Description

| | |
|--------------------|---|
| <i>slot-number</i> | (Optional) Slot number containing the line card about which to display CEF-related information. When you omit this argument, information about all line cards is displayed. |
| detail | (Optional) Displays detailed CEF information for the specified line card. |
| internal | (Optional) Displays internal CEF information for the specified line card. |

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|----------------------|--|
| 11.2 GS | This command was introduced to support the Cisco 12012 Internet router. |
| 11.1 CC | Multiple platform support was added. |
| 12.0(10)S | Output display was changed. |
| 12.1(2)T | This command was integrated into Cisco IOS Release 12.1(2)T. |
| 12.0(22)S, 12.2(14)S | The display output for this command was modified to include support for CEF for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) line card information. |

Usage Guidelines

This command is available only on distributed switching platforms.

When you omit the *slot-number* argument, information about all line cards is displayed. When you omit the *slot-number* argument and include the **detail** keyword, detailed information is displayed for all line cards. When you omit the *slot-number* argument and include the **internal** keyword, detailed internal information is displayed for all line cards. When you omit all keywords and arguments, the **show cef linecard** command displays important information about all line cards in table format.

Examples

The following is sample output from the **show cef linecard detail** command for all line cards:

```
Router# show cef linecard detail

CEF linecard slot number 0, status up
Sequence number 4, Maximum sequence number expected 28, Seq Epoch 2
Send failed 0, Out Of Sequence 0, drops 0
Linecard CEF reset 0, reloaded 1
95 elements packed in 6 messages(3588 bytes) sent
69 elements cleared
```



```

linecard in sync after reloading
0/0/0 xdr elements in LowQ/MediumQ/HighQ
11/9/69 peak elements on LowQ/MediumQ/HighQ
Input  packets 0, bytes 0
Output packets 0, bytes 0, drops 0
CEF Table statistics:
Table name          Version Prefix-xdr Status
Default-table       7          4 Active, up, sync
CEF linecard slot number 1, status up
Sequence number 4, Maximum sequence number expected 28, Seq Epoch 2
Send failed 0, Out Of Sequence 0, drops 0
Linecard CEF reset 0, reloaded 1
95 elements packed in 6 messages(3588 bytes) sent
69 elements cleared
linecard in sync after reloading
0/0/0 xdr elements in LowQ/MediumQ/HighQ
11/9/69 peak elements on LowQ/MediumQ/HighQ
Input  packets 0, bytes 0
Output packets 0, bytes 0, drops 0
CEF Table statistics:
Table name          Version Prefix-xdr Status
Default-table       7          4 Active, up, sync

```

The following is sample output from the **show cef linecard internal** command for all line cards:

```

Router# show cef linecard internal

CEF linecard slot number 0, status up
Sequence number 11, Maximum sequence number expected 35
Send failed 0, Out Of Sequence 0
Linecard CEF reset 2, reloaded 2
Total elements queued:
prefix                4
adjacency             4
interface             91
address              2
policy routing        2
hw interface          57
state                 6
resequence            2
control               13
table                 2
time                  4484
flow features deactivate 2
flow cache config     2
flow export config    2
dss                   2
isl                   2
mpls atm vc remove    2
mpls atm vc set label 2
                     2
                     2
                     3
                     1
4574 elements packed in 4495 messages(90286 bytes) sent
115 elements cleared
Total elements cleared:
prefix                2
adjacency             1
interface             63
address              1
policy routing        1
hw interface          29
state                 2

```

```

control                    5
table                     1
flow features deactivate  1
flow cache config         1
flow export config        1
dss                       1
isl                       1
mpls atm vc remove        1
mpls atm vc set label     1
                           1
                           1
                           1
linecard disabled - failed a reload
0/0/0 xdr elements in LowQ/MediumQ/HighQ
Input  packets 0, bytes 0
Output packets 0, bytes 0, drops 0

CEF Table statistics:
Table name                Version Prefix-xdr Status
Default-table              8          4 Active, sync

```

The following is sample output from the **show cef linecard** command. The command displays information for all line cards in table format.

```

Router# show cef linecard

Slot    MsgSent    XDRSent    Window    LowQ    MedQ    HighQ    Flags
0        6          95         24         0        0        0 up
1        6          95         24         0        0        0 up
VRF Default-table, version 8, 6 routes
Slot Version    CEF-XDR    I/Fs State    Flags
0        7          4          8 Active    up, sync
1        7          4         10 Active    up, sync

```

Table 48 describes the significant fields shown in the displays.

Table 48 *show cef linecard Field Descriptions*

| Field | Description |
|-----------------|--|
| Table name | Name of the CEF table. |
| Version | Number of the Forwarding Information Base (FIB) table version. |
| Prefix-xdr | Number of prefix IPC information elements XDRs processed. |
| Status | State of the CEF table. |
| Slot | Slot number of the line card. |
| MsgSent | Number of IPC messages sent. |
| XDRSent | XDRs packed into IPC messages sent from the Route Processor (RP) to the line card. |
| Window | Size of the IPC window between the line card and the RP. |
| LowQ/MedQ/HighQ | Number of XDR elements in the Low, Medium, and High priority queues. |

Table 48 *show cef linecard Field Descriptions (continued)*

| Field | Description |
|---------|---|
| Flags | Indicates the status of the line card. States are... <ul style="list-style-type: none"> • up—Line card is up. • sync—Line card is in synchronization with the main FIB. • FIB is repopulated on the line card. • reset—Line card FIB is reset. • reloading—Line card FIB is being reloaded. • disabled—Line card is disabled. |
| CEF-XDR | Number of CEF XDR messages processed. |
| I/Fs | Interface numbers. |

Related Commands

| Command | Description |
|---------------------------|---|
| show cef | Displays which packets the line cards dropped or displays which packets were not express-forwarded. |
| show cef interface | Displays CEF-related interface information. |
| show ipv6 cef | Displays entries in the IPv6 FIB. |

show clns neighbors

To display end system (ES), intermediate system (IS), and multitopology Integrated Intermediate System-to-Intermediate System (M-ISIS) neighbors, use the **show clns neighbors** command in user EXEC or privileged EXEC mode.

show clns [*area-tag*] **neighbors** [*interface-type interface-number*] [**area**] [**detail**]

Syntax Description

| | |
|-------------------------|--|
| <i>area-tag</i> | (Optional) This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. If an area tag is not specified, a null tag is assumed and the process is referenced with a null tag. If an area tag is specified, output is limited to the specified area. |
| <i>interface-type</i> | (Optional) Interface type. |
| <i>interface-number</i> | (Optional) Interface number. |
| area | (Optional) When specified, displays the CLNS multiarea adjacencies. |
| detail | (Optional) When specified, displays the area addresses advertised by the neighbor in the hello messages. Otherwise, a summary display is provided. In IPv6, displays the address family of the adjacency. |

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 10.0 | This command was introduced. |
| 12.0(5)T | The area and detail keywords were added. |
| 12.2(15)T | Support was added for IPv6. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

The **show clns neighbors** command displays the adjacency that is learned through multitopology IS-IS for IPv6.

Examples

The following is sample output from the **show clns neighbors** command:

Router# **show clns neighbors detail**

| System Id | Interface | SNPA | State | Holdtime | Type | Protocol |
|----------------|-----------|----------------|-------|----------|------|----------|
| 0000.0000.0007 | Et3/3 | aa00.0400.6408 | UP | 26 | L1 | IS-IS |
| 0000.0C00.0C35 | Et3/2 | 0000.0c00.0c36 | Up | 91 | L1 | IS-IS |
| 0800.2B16.24EA | Et3/3 | aa00.0400.2d05 | Up | 27 | L1 | M-ISIS |
| 0800.2B14.060E | Et3/2 | aa00.0400.9205 | Up | 8 | L1 | IS-IS |

The following is sample output from the **show clns neighbors** command using the **detail** keyword:

Router# **show clns neighbors detail**

```

System Id      Interface  SNPA      State  Holdtime  Type  Protocol
0000.0000.0007 Et3/3      aa00.0400.6408 Up      26      L1    IS-IS
Area Address(es): 20
IP Address(es): 192.16.0.42*
Uptime: 00:21:49
0000.0C00.0C35 Et3/2      0000.0c00.0c36 Up      91      L1    IS-IS
Area Address(es): 20
IP Address(es): 192.168.0.42*
Uptime: 00:21:52
0800.2B16.24EA Et3/3      aa00.0400.2d05 Up      27      L1    M-ISIS
Area Address(es): 20
IP Address(es): 192.168.0.42*
IPv6 Address(es): FE80::2B0:8EFF:FE31:EC57
Uptime: 00:00:27
Topology: IPv6
0800.2B14.060E Et3/2      aa00.0400.9205 Up      8       L1    IS-IS
Area Address(es): 20
IP Address(es): 192.168.0.30*
Uptime: 00:21:52

```

Table 49 describes the significant fields shown in the display.

Table 49 *show clns neighbors Field Descriptions*

| Field | Description |
|-----------|---|
| System Id | Six-byte value that identifies a system in an area. |
| Interface | Interface from which the system was learned. |
| SNPA | Subnetwork Point of Attachment. This is the data-link address. |
| State | State of the ES, IS, or M-ISIS. |
| Init | System is an IS and is waiting for an IS-IS hello message. IS-IS regards the neighbor as not adjacent. |
| Up | Believes the ES or IS is reachable. |
| Holdtime | Number of seconds before this adjacency entry times out. |
| Type | The adjacency type. Possible values are as follows: <ul style="list-style-type: none"> ES—End-system adjacency either discovered via the ES-IS protocol or statically configured. IS—Router adjacency either discovered via the ES-IS protocol or statically configured. M-ISIS—Router adjacency discovered via the multipoint IS-IS protocol. L1—Router adjacency for Level 1 routing only. L1L2—Router adjacency for Level 1 and Level 2 routing. L2—Router adjacency for Level 2 only. |
| Protocol | Protocol through which the adjacency was learned. Valid protocol sources are ES-IS, IS-IS, ISO IGRP, Static, DECnet, and M-ISIS. |

Notice that the information displayed in the **show clns neighbors detail** command output includes everything shown in **show clns neighbors** command output in addition to the area address associated with the IS neighbor and its uptime. When IP routing is enabled, Integrated-ISIS adds information to the output of the **show clns** commands. The **show clns neighbors detail** command output shows the IP addresses that are defined for the directly connected interface and an asterisk (*) to indicate which IP address is the next hop.

show crypto ipsec policy

To display the parameters for each IP Security (IPSec) policy, use the **show crypto ipsec policy** command in user EXEC or privileged EXEC mode.

show crypto ipsec policy [**name** *policy-name*]

Syntax Description

name *policy-name* (Optional) The specific policy for which parameters will be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|----------|------------------------------|
| 12.3(4)T | This command was introduced. |

Usage Guidelines

If no policy is specified, then information about all policies is displayed.

Examples

The following is sample output from the **show crypto ipsec policy** command:

```
Router# show crypto ipsec policy

Crypto IPsec client security policy data

Policy name:      OSPFv3-1-1000
Policy refcount:  1
Inbound  AH SPI:  1000 (0x3E8)
Outbound AH SPI:  1000 (0x3E8)
Inbound  AH Key:  1234567890ABCDEF1234567890ABCDEF
Outbound AH Key:  1234567890ABCDEF1234567890ABCDEF
Transform set:    ah-md5-hmac
```

Table 50 describes the significant fields shown in the display.

Table 50 *show crypto ipsec policy Field Descriptions*

| Field | Description |
|-----------------|---|
| Policy name | Specifies the name of the policy. |
| Inbound AH SPI | The authentication header (AH) security policy index (SPI) for inbound links. |
| Outbound AH SPI | The AH SPI for outbound links. |
| Inbound AH Key | The AH key for inbound links. |
| Outbound AH Key | The AH key for outbound links. |
| Transform set | The transform set, which is an acceptable combination of security protocols and algorithms. |

show crypto ipsec sa ipv6

To display the settings used by current security associations (SAs), use the **show crypto ipsec sa ipv6** command in user EXEC or privileged EXEC mode.

```
show crypto ipsec sa ipv6 [interface-type interface-number] [detailed]
```

| | | |
|--------------------|-------------------------|--|
| Syntax Description | <i>interface-type</i> | (Optional) Interface type. |
| | <i>interface-number</i> | (Optional) Interface number. |
| | detailed | (Optional) Displays detailed SA information. |

| | |
|---------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| | | |
|-----------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 12.3(4)T | This command was introduced. |

| | |
|------------------|---|
| Usage Guidelines | If no keyword is used, all SAs are displayed. They are sorted first by interface, and then by traffic flow (for example, source or destination address, mask, protocol, or port). Within a flow, the SAs are listed by protocol (Authentication Header [AH] or Encapsulating Security Payload [ESP]) and direction (inbound or outbound). |
|------------------|---|

Examples The following is sample output from the **show crypto ipsec sa ipv6** command:

```
Router# show crypto ipsec sa ipv6

IPv6 IPsec SA info for interface Ethernet0/0

protected policy name:OSPFv3-1-1000
IPsec created ACL name:Ethernet0/0-ipsecv6-ACL

local ident (addr/prefixlen/proto/port):(FE80::/10/89/0)
remote ident (addr/prefixlen/proto/port):(::/0/89/0)
current_peer::
  PERMIT, flags={origin_is_acl,}
  #pkts encaps:21, #pkts encrypt:0, #pkts digest:21
  #pkts decaps:20, #pkts decrypt:0, #pkts verify:20
  #pkts compressed:0, #pkts decompressed:0
  #pkts not compressed:0, #pkts compr. failed:0
  #pkts not decompressed:0, #pkts decompress failed:0
  #send errors 0, #recv errors 0

local crypto endpt. ::, remote crypto endpt. ::
path mtu 1500, media mtu 1500
current outbound spi:0x3E8(1000)

inbound ESP SAs:

inbound AH SAs:
```



```
spi:0x3E8(1000)
  transform:ah-md5-hmac ,
  in use settings ={Transport, }
  slot:0, conn_id:2000, flow_id:1, crypto map:N/R
  no sa timing (manual-keyed)
  replay detection support:N
```

inbound PCP SAs:

outbound ESP SAs:

outbound AH SAs:

```
spi:0x3E8(1000)
  transform:ah-md5-hmac ,
  in use settings ={Transport, }
  slot:0, conn_id:2001, flow_id:2, crypto map:N/R
  no sa timing (manual-keyed)
  replay detection support:N
```

outbound PCP SAs:

show frame-relay map

To display the current map entries and information about the connections, use the **show frame-relay map** command in EXEC mode.

show frame-relay map

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

| | |
|----------------------|------|
| Command Modes | EXEC |
|----------------------|------|

| Command History | Release | Modification |
|-----------------|--|---|
| | 10.0 | This command was introduced. |
| | 12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S | The display output for this command was modified to include the IPv6 address mappings of remote nodes to Frame Relay permanent virtual circuits (PVCs). |

| | |
|-----------------|--|
| Examples | The following is sample output from the show frame-relay map command: |
|-----------------|--|

```
Router# show frame-relay map
```

```
Serial 1 (administratively down): ip 10.108.177.177 dlci 177 (0xB1,0x2C10), static,
broadcast, CISCO, TCP/IP Header Compression (inherited), passive (inherited)
```

The following sample output from the **show frame-relay map** command shows that the link-local and global IPv6 addresses (FE80::E0:F727:E400:A and 2001:0DB8:2222::73; FE80::60:3E47:AC8:8 and 2001:0DB8:2222::72) of two remote nodes are explicitly mapped to data-link connection identifier (DLCI) 17 and DLCI 19, respectively. Both DLCI 17 and DLCI 19 are terminated on interface serial 3 of this node; therefore, interface serial 3 of this node is a point-to-multipoint interface.

```
Router# show frame-relay map
```

```
Serial3 (up): ipv6 FE80::E0:F727:E400:A dlci 17(0x11,0x410), static,
                broadcast, CISCO, status defined, active
Serial3 (up): ipv6 2001:0DB8:2222::72 dlci 19(0x13,0x430), static,
                CISCO, status defined, active
Serial3 (up): ipv6 2001:0DB8:2222::73 dlci 17(0x11,0x410), static,
                CISCO, status defined, active
Serial3 (up): ipv6 FE80::60:3E47:AC8:8 dlci 19(0x13,0x430), static,
                broadcast, CISCO, status defined, active
```

Table 51 describes the significant fields shown in the displays.

Table 51 show frame-relay map Field Descriptions

| Field | Description |
|----------------------------------|---|
| Serial 1 (administratively down) | Identifies a Frame Relay interface and its status (up or down). |
| ip 10.108.177.177 | Destination IP address. |

Table 51 *show frame-relay map Field Descriptions (continued)*

| Field | Description |
|--|--|
| dlci 177 (0xB1,0x2C10) | DLCI that identifies the logical connection being used to reach this interface. This value is displayed in three ways: its decimal value (177), its hexadecimal value (0xB1), and its value as it would appear on the wire (0x2C10). |
| static | Indicates whether this is a static or dynamic entry. |
| broadcast | Indicates pseudobroadcasting. |
| CISCO | Indicates the encapsulation type for this map; either CISCO or IETF. |
| status defined, active | Indicates that the mapping between the destination address and the data-link connection identifier (DLCI) used to connect to the destination address is active. |
| TCP/IP Header Compression (inherited), passive (inherited) | Indicates whether the TCP/IP header compression characteristics were inherited from the interface or were explicitly configured for the IP map. |

Related Commands

| Command | Description |
|-----------------------------|--|
| show frame-relay pvc | Displays statistics about PVCs for Frame Relay interfaces. |

show ip sockets

To display IP socket information, use the **show ip sockets** command in user EXEC or privileged EXEC mode.

show ip sockets

Syntax Description This command has no keywords or arguments.

Defaults No default behavior or values.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|--|---|
| | 10.0 T | This command was introduced. |
| | 12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S | Support for IPv6 socket information in the display output of the command was added. |

Examples The following is sample output from the **show ip sockets** command:

```
Router# show ip sockets

Proto    Remote      Port      Local      Port    In  Out  Stat  TTY  OutputIF
  17      0.0.0.0        0      9.2.64.5    67     0   0   489   0
  17      --listen--      --any--    521     0   0   401   0
```

Table 52 describes the significant fields shown in the display.

Table 52 show ip sockets Field Descriptions

| Field | Description |
|--------|---|
| Proto | Protocol type, for example, User Datagram Protocol (UDP) or TCP. |
| Remote | Remote address connected to this networking device. If the remote address is considered illegal, “--listen--” is displayed. |
| Port | Remote port. If the remote address is considered illegal, “--listen--” is displayed. |
| Local | Local address. If the local address is considered illegal or is the address 0.0.0.0, “--any--” displays. |
| Port | Local port. |
| In | Input queue size. |
| Out | Output queue size. |
| Stat | Various statistics for a socket. |

Table 52 *show ip sockets Field Descriptions (continued)*

| Field | Description |
|----------|--|
| TTY | The tty number for the creator of this socket. |
| OutputIF | Output IF string, if one exists. |

show ipv6 access-list

To display the contents of all current IPv6 access lists, use the **show ipv6 access-list** command in user EXEC or privileged EXEC mode.

show ipv6 access-list [*access-list-name*]

Syntax Description

| | |
|-------------------------|---------------------------------|
| <i>access-list-name</i> | (Optional) Name of access list. |
|-------------------------|---------------------------------|

Defaults

Displays all IPv6 access lists.

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|----------------------|--|
| 12.2(2)T | This command was introduced. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.0(23)S, 12.2(13)T | The priority field was changed to sequence and Layer 4 protocol information (extended IPv6 access list functionality) was added to the display output. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **show ipv6 access-list** command provides output similar to the **show ip access-list** command, except that it is IPv6-specific.

Examples

The following output from the **show ipv6 access-list** command shows IPv6 access lists named inbound, tcptraffic, and outbound:

```
Router# show ipv6 access-list
```

```
IPv6 access list inbound
```

```
  permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
  permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
  permit udp any any reflect udptraffic sequence 30
```

```
IPv6 access list tcptraffic (reflexive) (per-user)
```

```
  permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
    left 243) sequence 1
  permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
    (time left 296) sequence 2
```

```
IPv6 access list outbound
```

```
  evaluate udptraffic
  evaluate tcptraffic
```

Table 53 describes the significant fields shown in the display.

Table 53 *show ipv6 access-list Field Descriptions*

| Field | Description |
|--------------------------|--|
| ipv6 access list inbound | Name of the IPv6 access list, for example, inbound. |
| permit | Permits any packet that matches the specified protocol type. |
| tcp | Transmission Control Protocol. The higher-level (Layer 4) protocol type that the packet must match. |
| any | Equal to ::/0. |
| eq | An equal operand that compares the source or destination ports of TCP or UDP packets. |
| bgp | Border Gateway Protocol. The lower-level (Layer 3) protocol type that the packet must be equal to. |
| reflect | Indicates a reflexive IPv6 access list. |
| tcptraffic (8 matches) | The name of the reflexive IPv6 access list and the number of matches for the access list. The clear ipv6 access-list privileged EXEC command resets the IPv6 access list match counters. |
| sequence 10 | Sequence in which an incoming packet is compared to lines in an access list. Lines in an access list are ordered from first priority (lowest number, for example, 10) to last priority (highest number, for example, 80). |
| host 2001:0DB8:1::1 | The source IPv6 host address that the source address of the packet must match. |
| host 2001:0DB8:1::2 | The destination IPv6 host address that the destination address of the packet must match. |
| 11000 | The ephemeral source port number for the outgoing connection. |
| timeout 300 | The total interval of idle time (in seconds) after which the temporary IPv6 reflexive access list named tcptraffic will time out for the indicated session. |
| (time left 243) | The amount of idle time (in seconds) remaining before the temporary IPv6 reflexive access list named tcptraffic is deleted for the indicated session. Additional received traffic that matches the indicated session resets this value to 300 seconds. |
| evaluate udptraffic | Indicates the IPv6 reflexive access list named udptraffic is nested in the IPv6 access list named outbound. |

Related Commands

| Command | Description |
|-------------------------------|---|
| clear ipv6 access-list | Resets the IPv6 access list match counters. |
| show ip access-list | Displays the contents of all current IP access lists. |
| show ip prefix-list | Displays information about a prefix list or prefix list entries. |
| show ipv6 prefix-list | Displays information about an IPv6 prefix list or IPv6 prefix list entries. |

show ipv6 cef

To display entries in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef** command in user EXEC or privileged EXEC mode.

```
show ipv6 cef [interface-type interface-number] [ipv6-prefix/prefix-length] [longer-prefixes]  
[detail]
```

Syntax Description

| | |
|-------------------------|---|
| <i>interface-type</i> | (Optional) Interface type for which to display FIB entries. |
| <i>interface-number</i> | (Optional) Interface number for which to display FIB entries. |
| <i>ipv6-prefix</i> | (Optional) The IPv6 network assigned to the interface. 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> | (Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |
| longer-prefixes | (Optional) Displays FIB entries for more specific destinations. |
| detail | (Optional) Displays detailed FIB entry information. |

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|------------|--|
| 12.0(21)ST | This command was introduced. |
| 12.0(22)S | The <i>interface-type</i> and <i>interface-number</i> arguments, and the longer-prefixes and detail keywords, were added. MPLS label information was added to the display. This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **show ipv6 cef** command is similar to the **show ip cef** command, except that it is IPv6-specific.

The **show ipv6 cef** command without any keywords or arguments shows a brief display of all FIB entries.

The **show ipv6 cef detail** command shows detailed information for all FIB entries.

Examples

The following is sample output from the **show ipv6 cef** command when no keywords or arguments are entered:


```

Router# show ipv6 cef

Global IPv6 CEF Table
12 prefixes

2FFE::3/128
    Receive
2FFE::/64
    attached to POS3/1
3FFE::/64
    nexthop FE80::yyyy:4AFF:FE6D:B980 POS3/1
    nexthop FE80::xxxx:7DFF:FE8D:A840 FastEthernet1/0
3FFE:zz::3/128
    Receive
3FFE:zz::/64
    attached to FastEthernet1/0
3FFE:rr::3/128
    Receive
3FFE:rr::/64
    attached to FastEthernet1/1
3FFE:pp::3/128
    Receive
3FFE:pp::/64
    attached to FastEthernet1/2
3FFE:nnnn:2222::/64
    nexthop::POS3/1
3FFE:ssss::/64
    recursive via 2FFE::2 POS3/1
FE80::/64
    Receive

```

The following is sample output from the **show ipv6 cef detail** command for Fast Ethernet interface 1/0:

```

Router# show ipv6 cef fastethernet1/0 detail

IPv6 CEF is enabled and running
IPv6 CEF default table
2 prefixes
3FFE:zz::/64
    attached to FastEthernet1/0
3FFE:rr::/64
    attached to FastEthernet1/1

```

The following is sample output from the **show ipv6 cef longer-prefixes detail** command for the IPv6 prefix 3FFE:xxxx:20:1::12/128.

```

Router# show ipv6 cef 3FFE:xxxx:20:1::12/128 longer-prefixes detail

IPv6 CEF is enabled and running
IPv6 CEF default table
2 prefixes
3FFE:xxxx:20:1::12/128 Receive
    Receive
3FFE:xxxx:20:1::/64 Attached, Connected
    attached to Tunnel81

```

Table 54 describes the significant fields shown in the display.

Table 54 *show ipv6 cef Field Descriptions*

| Field | Description |
|--|--|
| 12 prefixes | Indicates the total number of IPv6 prefixes in the CEF table. |
| 2FFE::3/128 | Indicates the IPv6 prefix of the remote network. |
| Receive | Indicates that this IPv6 prefix is local to the router. |
| 3FFE::/64 | Indicates that IPv6 prefix 3FFE::/64 is reachable through these next-hop addresses and interfaces. Multiple next-hop entries are shown for IPv6 prefixes that have load sharing. |
| nexthop FE80::yyyy:4AFF:FE6D:B980 POS3/1 | |
| nexthop FE80::xxxx:7DFF:FE8D:A840 FastEthernet1/0 | |
| attached to FastEthernet1/0 | Indicates that this IPv6 prefix is a connected network on Fast Ethernet interface 1/0. |
| recursive via 2FFE::2 POS3/1 | Indicates that this IPv6 prefix uses the same forwarding information as 2FFE::2 POS3/1. |

The following is sample output from the **show ipv6 cef** command, showing information about the Multiprotocol Label Switching (MPLS) labels associated with the FIB table entries for an IPv6 prefix that is configured to be an IPv6 provider edge router (Cisco 6PE) using MPLS to transport IPv6 traffic over an IPv4 network.

To display label information from the CEF table, enter the **show ipv6 cef EXEC** command with an IPv6 prefix:

```
Router# show ipv6 cef 2001:0DB8::/32

2001:0DB8::/32
  nexthop ::FFFF:192.168.99.70
  fast tag rewrite with Se0/0, point2point, tags imposed {19 20}
```

Related Commands

| Command | Description |
|--------------------------------|--|
| show cef interface | Displays CEF-related interface information. |
| show ipv6 cef adjacency | Displays CEFv6 recursive and direct prefixes resolved through an adjacency. |
| show ipv6 route | Displays IPv6 router advertisement information received from onlink routers. |

show ipv6 cef adjacency

To display Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) recursive and direct prefixes resolved through an adjacency, use the **show ipv6 cef adjacency** command in user EXEC or privileged EXEC mode.

show ipv6 cef adjacency *interface-type interface-number ipv6-address* [**detail**]

To display CEFv6 and dCEFv6 recursive and direct prefixes resolved through special adjacency types representing nonstandard switching paths, use this form of the **show ip cef adjacency** command in user EXEC or privileged EXEC mode.

show ipv6 cef adjacency {**discard** | **drop** | **glean** | **null** | **punt**} [**detail**]

Syntax Description

| | |
|-------------------------|--|
| <i>interface-type</i> | Interface type for which to display Forwarding Information Base (FIB) entries. |
| <i>interface-number</i> | Interface number for which to display FIB entries. |
| <i>ipv6-address</i> | Next-hop IPv6 address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| detail | (Optional) Displays detailed information for each CEFv6 adjacency type entry. |
| discard | Discard adjacency. Sets up for loopback interfaces. Loopback IPv6 addresses are receive entries in the FIB table. |
| drop | Drop adjacency. Packets forwarded to this adjacency are dropped. |
| glean | Glean adjacency. Represents destinations on a connected interface for which no Address Resolution Protocol (ARP) cache entry exists. |
| null | Null adjacency. Formed for the null 0 interface. Packets forwarded to this adjacency are dropped. |
| punt | Punt adjacency. Represents destinations that cannot be switched in the normal path and that are punted to the next fastest switching vector. |

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.0(22)S | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **show ipv6 cef adjacency** command is similar to the **show ip cef adjacency** command, except that it is IPv6-specific.

An adjacency is a node that can be reached by one Layer 2 hop.

Examples

This command shows all prefixes resolved through a regular next-hop adjacency or through a special adjacency type such as discard, drop, glean, null, and punt.

The following is sample output from the **show ipv6 cef adjacency** command when the **glean** type is specified:

```
Router# show ipv6 cef adjacency glean

Prefix          Next Hop          Interface
3FFE:xxxx::/24   attached          Ethernet1
2002::/16        3FFE:xxxx::1      Ethernet1
```

The following is sample output from the **show ipv6 cef adjacency drop** command with **detail** specified:

```
Router# show ipv6 cef adjacency drop detail

IPv6 CEF is enabled and running
IPv6 CEF default table
12 prefixes
```

The following sample output shows the direct IPv6 prefix when next-hop Ethernet interface 1 is specified:

```
Router# show ipv6 cef adjacency ethernet 1 3FFE:xxxx::250:8BFF:FEE8:F800

Prefix          Next Hop          Interface
3FFE:xxxx::250:8BFF:FEE8:F800/128  2002::/16         Ethernet1
```

Table 55 describes the significant fields shown in the display.

Table 55 *show ipv6 cef adjacency Field Descriptions*

| Field | Description |
|-----------|--------------------------|
| Prefix | Destination IPv6 prefix. |
| Next Hop | Next-hop IPv6 address. |
| Interface | Next-hop interface. |

Related Commands

| Command | Description |
|------------------------------|--|
| show ipv6 cef summary | Displays a summary of the entries in the IPv6 FIB. |

show ipv6 cef non-recursive

To display nonrecursive route entries in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef non-recursive** command in user EXEC or privileged EXEC mode.

show ipv6 cef non-recursive [detail]

| | |
|---------------------------|---|
| Syntax Description | detail (Optional) Displays detailed FIB entry information. |
|---------------------------|---|

| | |
|----------------------|------------------------------|
| Command Modes | User EXEC Privileged EXEC |
|----------------------|------------------------------|

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.0(22)S | This command was introduced. |
| | 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

| | |
|-------------------------|---|
| Usage Guidelines | <p>The show ipv6 cef non-recursive command is similar to the show ip cef non-recursive command, except that it is IPv6-specific.</p> <p>The show ipv6 cef non-recursive detail command shows detailed FIB entry information for all nonrecursive routes.</p> |
|-------------------------|---|

| | |
|-----------------|--|
| Examples | The following is sample output from the show ipv6 cef non-recursive detail command: |
|-----------------|--|

```
Router# show ipv6 cef non-recursive detail

IPv6 CEF is enabled and running
IPv6 CEF default table
8 prefixes
2001:xx::/35
    nexthop FE80::ssss:CFF:FE3D:DCC9 Tunnel155
2001:zzz:500::/40
    nexthop FE80::nnnn:801A Tunnel32
2001:zzz::/35
    nexthop 3FFE:mmm:8023:21::2 Tunnel26
3FFE:yyy:8023:37::1/128 Receive
    Receive
3FFE:yyy:8023:37::/64 Attached, Connected
    attached to Tunnel37
3FFE:yyy:8023:38::1/128 Receive
    Receive
3FFE:yyy:8023:38::/64 Attached, Connected
    attached to Tunnel40
3FFE:yyy:8023:39::1/128 Receive
    Receive
```

Table 56 describes the significant fields shown in the display.

Table 56 *show ipv6 cef non-recursive Field Descriptions*

| Field | Description |
|--|--|
| 8 prefixes | Indicates the total number of IPv6 prefixes in the CEF table. |
| 2001:xx::/35 | Indicates the IPv6 prefix of the remote network. |
| 2001:zzz:500::/40 nexthop FE80::nnnn:801A Tunnel32 | Indicates that IPv6 prefix 2001:zzz:500::/40 is reachable through this next-hop address and interface. |
| attached to Tunnel37 | Indicates that this IPv6 prefix is a connected network on Tunnel interface 37. |
| Receive | Indicates that this IPv6 prefix is local to the router. |

Related Commands

| Command | Description |
|---------------------------------|---|
| show ipv6 cef | Displays entries in the IPv6 FIB. |
| show ipv6 cef summary | Displays a summary of the entries in the IPv6 forwarding FIB. |
| show ipv6 cef unresolved | Displays unresolved entries in the IPv6 FIB. |

show ipv6 cef summary

To display a summary of the entries in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef summary** command in user EXEC or privileged EXEC mode.

show ipv6 cef summary

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(22)S | This command was introduced. |
| | 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines The **show ipv6 cef summary** command is similar to the **show ip cef summary** command, except that it is IPv6-specific.

Examples The following is sample output from the **show ipv6 cef summary** command:

```
Router# show ipv6 cef summary
```

```
IPv6 CEF is enabled and running
Slow processing intvl = 1 seconds backoff level current/max 0/0
0 unresolved prefixes, 0 requiring adjacency update
IPv6 CEF default table
9 prefixes
```

Table 57 describes the significant fields shown in the display.

Table 57 *show ipv6 cef summary Field Descriptions*

| Field | Description |
|----------------------------|--|
| Slow processing intvl | Indicates the waiting time (in seconds) before the software attempts to resolve any unresolved routes. |
| unresolved prefixes | Indicates the number of unresolved routes. |
| requiring adjacency update | Indicates the number of prefixes that have been resolved but the associated forwarding information has not yet been updated to reflect the route resolution. |

| Related Commands | Command | Description |
|------------------|--------------------|---|
| | show ipv6 cef | Displays entries in the IPv6 FIB. |
| | show cef interface | Displays CEF-related interface information. |

show ipv6 cef traffic prefix-length

To display Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) traffic statistics, use the **show ipv6 cef traffic prefix-length** command in user EXEC or privileged EXEC mode.

show ipv6 cef traffic prefix-length

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(22)S | This command was introduced. |
| | 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines The **show ipv6 cef traffic prefix-length** command is similar to the **show ip cef traffic prefix-length** command, except that it is IPv6-specific.

This command is used to display CEFv6 switched traffic statistics by destination prefix length. The **ipv6 cef accounting prefix-length** command must be enabled for the counters to increment.

Examples The following is sample output from the **show ipv6 cef traffic prefix-length** command:

```
Router# show ipv6 cef traffic prefix-length
```

```
IPv6 prefix length switching statistics:
```

| Prefix Length | Number of Packets | Number of Bytes |
|---------------|-------------------|-----------------|
| 0 | 0 | 0 |
| 1 | 24 | 3840 |
| 2 | 0 | 0 |
| 3 | 14 | 1120 |
| 4 | 0 | 0 |
| 5 | 10 | 1200 |
| . | | |
| . | | |
| . | | |
| 28 | 0 | 0 |
| 29 | 4 | 512 |
| 30 | 0 | 0 |
| 31 | 18 | 2448 |
| 32 | 0 | 0 |

Table 58 describes the significant fields shown in the display.

Table 58 *show ipv6 cef traffic prefix-length Field Descriptions*

| Field | Description |
|-------------------|---|
| Prefix Length | Destination IPv6 prefix length for CEF switched traffic. |
| Number of Packets | Number of packets forwarded for the specified IPv6 prefix length. |
| Number of Bytes | Number of bytes sent for the specified IPv6 prefix length. |

Related Commands

| Command | Description |
|------------------------------|--|
| ipv6 cef accounting | Enables CEFv6 network accounting. |
| show ipv6 cef | Displays entries in the IPv6 FIB. |
| show ipv6 cef summary | Displays a summary of the entries in the IPv6 FIB. |

show ipv6 cef unresolved

To display unresolved entries in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef unresolved** command in user EXEC or privileged EXEC mode.

show ipv6 cef unresolved [detail]

| | | |
|--------------------|--|---|
| Syntax Description | detail (Optional) Displays detailed FIB entry information. | |
| Command Modes | User EXEC Privileged EXEC | |
| Command History | Release | Modification |
| | 12.0(22)S | This command was introduced. |
| | 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| Usage Guidelines | <p>The show ipv6 cef unresolved command is similar to the show ip cef unresolved command, except that it is IPv6-specific.</p> <p>The show ipv6 cef unresolved detail command displays detailed information for all unresolved FIB entries.</p> | |
| Related Commands | Command | Description |
| | show cef interface | Displays CEF-related interface information. |
| | show ipv6 cef | Displays entries in the IPv6 FIB. |
| | show ipv6 cef summary | Displays a summary of the entries in the IPv6 FIB. |

show ipv6 dhcp

To display the Dynamic Host Configuration Protocol (DHCP) unique identifier (DUID) on a specified device, use the **show ipv6 dhcp** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp

Syntax Description This command has no keywords or arguments.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.3(4)T | This command was introduced. |

Usage Guidelines This implementation uses the DUID based on the link-layer address for both client and server identifiers. The device uses the MAC address from the lowest-numbered interface to form the DUID. The network interface is assumed to be permanently attached to the device. Use the **show ipv6 dhcp** command to display the DUID of a device.

Examples The following is sample output from the **show ipv6 dhcp** command:

```
Router# show ipv6 dhcp

This device's DHCPv6 unique identifier(DUID): 000300010002FCA5DC1C
```

show ipv6 dhcp binding

To display automatic client bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 server binding table, use the **show ipv6 dhcp binding** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp binding [*ipv6-address*]

| | | |
|---------------------------|---------------------|---|
| Syntax Description | <i>ipv6-address</i> | (Optional) The address of a DHCP for IPv6 client. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
|---------------------------|---------------------|---|

| | |
|----------------------|------------------------------|
| Command Modes | User EXEC Privileged EXEC |
|----------------------|------------------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 12.3(4)T | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | The show ipv6 dhcp binding command displays all automatic client bindings from the DHCP for IPv6 server binding table if the <i>ipv6-address</i> argument is not specified. When the <i>ipv6-address</i> argument is specified, only the binding for the specified client is displayed. |
|-------------------------|--|

| | |
|-----------------|--|
| Examples | The following is sample output from the show ipv6 dhcp binding command: |
|-----------------|--|

```
Router# show ipv6 dhcp binding

Client: FE80::202:FCFF:FEA5:DC39 (Ethernet2/1)
  DUID: 000300010002FCA5DC1C
  IA PD: IA ID 0x00040001, T1 0, T2 0
    Prefix: 3FFE:C00:C18:11::/68
           preferred lifetime 180, valid lifetime 12345
           expires at Nov 08 2002 02:24 PM (12320 seconds)
Client: FE80::202:FCFF:FEA5:C039 (Ethernet2/1)
  DUID: 000300010002FCA5C01C
  IA PD: IA ID 0x00040001, T1 0, T2 0
    Prefix: 3FFE:C00:C18:1::/72
           preferred lifetime 240, valid lifetime 54321
           expires at Nov 09 2002 02:02 AM (54246 seconds)
    Prefix: 3FFE:C00:C18:2::/72
           preferred lifetime 300, valid lifetime 54333
           expires at Nov 09 2002 02:03 AM (54258 seconds)
    Prefix: 3FFE:C00:C18:3::/72
           preferred lifetime 280, valid lifetime 51111
```

Table 59 describes the significant fields shown in the display.

Table 59 *show ipv6 dhcp binding Field Descriptions*

| Field | Description |
|------------------------------------|--|
| Client | Address of a specified client. |
| DUID | DHCP unique identifier (DUID). |
| IAPD | Identity association for prefix delegation (IAPD), which is a collection of prefixes assigned to a client. |
| IA ID | Identifier for this IAPD. |
| Prefix | Prefix(es) delegated to the indicated IAPD on the specified client. |
| preferred lifetime, valid lifetime | The preferred lifetime and valid lifetime settings for the specified client. |
| Expires at | Date and time at which the valid lifetime expires. |

Related Commands

| Command | Description |
|--------------------------------|---|
| clear ipv6 dhcp binding | Deletes automatic client bindings from the DHCP for IPv6 binding table. |

show ipv6 dhcp database

To display the Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent information, use the **show ipv6 dhcp database** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp database [*agent-URL*]

| | | |
|---------------------------|------------------|---|
| Syntax Description | <i>agent-URL</i> | (Optional) A Flash, NVRAM, FTP, TFTP, or Remote Copy Protocol (RCP) uniform resource locator. |
|---------------------------|------------------|---|

| | |
|----------------------|------------------------------|
| Command Modes | User EXEC Privileged EXEC |
|----------------------|------------------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 12.3(4)T | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | <p>Each permanent storage to which the binding database is saved is called the database agent. An agent can be configured using the ipv6 dhcp database command. Supported database agents include FTP and TFTP servers, RCP, Flash file system, and NVRAM.</p> <p>The show ipv6 dhcp database command displays DHCP for IPv6 binding database agent information. If the <i>agent-URL</i> argument is specified, only the specified agent is displayed. If the <i>agent-URL</i> argument is not specified, all database agents are shown.</p> |
|-------------------------|--|

| | |
|-----------------|---|
| Examples | The following is sample output from the show ipv6 dhcp database command: |
|-----------------|---|

```
Router# show ipv6 dhcp database

Database agent tftp://172.19.216.133/db.tftp:
  write delay: 69 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
    write timer expires in 56 seconds
  last read at Jan 06 2003 05:41 PM
  successful read times 1
  failed read times 0
  successful write times 3172
  failed write times 2
Database agent nvram:/dhcpv6-binding:
  write delay: 60 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
    write timer expires in 37 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 3325
  failed write times 0
Database agent flash:/dhcpv6-db:
  write delay: 82 seconds, transfer timeout: 3 seconds
  last written at Jan 09 2003 01:54 PM,
    write timer expires in 50 seconds
```

```

last read at never
successful read times 0
failed read times 0
successful write times 2220
failed write times 614

```

Table 60 describes the significant fields shown in the display.

Table 60 *show ipv6 dhcp database Field Descriptions*

| Field | Description |
|-------------------------------|--|
| Database agent | Specifies the database agent. |
| Write delay | The amount of time (in seconds) to wait before updating the database. |
| transfer timeout | Specifies how long (in seconds) the DHCP server should wait before aborting a database transfer. Transfers that exceed the timeout period are aborted. |
| Last written | The last date and time bindings were written to the file server. |
| Write timer expires... | The length of time, in seconds, before the write timer expires. |
| Last read | The last date and time bindings were read from the file server. |
| Successful/failed read times | The number of successful or failed read times. |
| Successful/failed write times | The number of successful or failed write times. |

Related Commands

| Command | Description |
|---------------------------|--|
| ipv6 dhcp database | Specifies DHCP for IPv6 binding database agent parameters. |

show ipv6 dhcp interface

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 interface information, use the **show ipv6 dhcp interface** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp interface [*interface-type interface-number*]

Syntax Description

| | |
|-------------------------|---|
| <i>interface-type</i> | (Optional) Interface type and number. For more information, use the |
| <i>interface-number</i> | question mark (?) online help function. |

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|----------|------------------------------|
| 12.3(4)T | This command was introduced. |

Usage Guidelines

If no interfaces are specified, all interfaces on which DHCP for IPv6 (client or server) is enabled are shown. If an interface is specified, only information about the specified interface is displayed.

Examples

The following is sample output from the **show ipv6 dhcp interface** command. In the first example, the command is used on a router that has an interface acting as a DHCP for IPv6 server. In the second example, the command is used on a router that has an interface acting as a DHCP for IPv6 client:

```
Router1# show ipv6 dhcp interface
```

```
Ethernet2/1 is in server mode
  Using pool: svr-p1
  Preference value: 20
  Rapid-Commit is disabled
```

```
Router2# show ipv6 dhcp interface
```

```
Ethernet2/1 is in client mode
  State is OPEN (1)
  List of known servers:
    Address: FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
    Preference: 20
    IA PD: IA ID 0x00040001, T1 120, T2 192
      Prefix: 3FFE:C00:C18:1::/72
        preferred lifetime 240, valid lifetime 54321
        expires at Nov 08 2002 09:10 AM (54319 seconds)
      Prefix: 3FFE:C00:C18:2::/72
        preferred lifetime 300, valid lifetime 54333
        expires at Nov 08 2002 09:11 AM (54331 seconds)
      Prefix: 3FFE:C00:C18:3::/72
        preferred lifetime 280, valid lifetime 51111
        expires at Nov 08 2002 08:17 AM (51109 seconds)
    DNS server: 1001::1
    DNS server: 1001::2
```

```

Domain name: domain1.net
Domain name: domain2.net
Domain name: domain3.net
Prefix name is cli-p1
Rapid-Commit is enabled

```

Table 61 describes the significant fields shown in the display.

Table 61 *show ipv6 dhcp interface Field Descriptions*

| Field | Description |
|--------------------------------------|---|
| Ethernet2/1 is in server/client mode | Displays whether the specified interface is in server or client mode. |
| Using pool: svr-p1 | The name of the pool that is being used by the interface. |
| State is OPEN | State of the DHCP for IPv6 client on this interface. “Open” indicates that configuration information has been received. |
| List of known servers | Lists the servers on the interface. |
| Address, DUID | Address and DHCP unique identifier (DUID) of a server heard on the specified interface. |
| Preference value: | The advertised (or default of 0) preference value for the indicated server. |
| Prefix name is cli-p1 | Displays the IPv6 general prefix pool name, in which prefixes successfully acquired on this interface are stored. |
| Rapid commit is disabled | Displays whether the rapid-commit keyword has been enabled on the interface. |

Related Commands

| Command | Description |
|----------------------------|---|
| ipv6 dhcp client pd | Enables the DHCP for IPv6 client process and enables request for prefix delegation through a specified interface. |
| ipv6 dhcp server | Enables DHCP for IPv6 service on an interface. |

show ipv6 dhcp pool

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 configuration pool information, use the **show ipv6 dhcp pool** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp pool [*poolname*]

| | | |
|---------------------------|-----------------|---|
| Syntax Description | <i>poolname</i> | (Optional) User-defined name for the local prefix pool. The pool name can be a symbolic string (such as “Engineering”) or an integer (such as 0). |
|---------------------------|-----------------|---|

| | |
|----------------------|------------------------------|
| Command Modes | User EXEC Privileged EXEC |
|----------------------|------------------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 12.3(4)T | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | <p>Use the ipv6 dhcp pool command to create a configuration pool, and use the ipv6 dhcp server command to associate the configuration pool with a server on an interface.</p> <p>The show ipv6 dhcp pool command displays DHCP for IPv6 configuration pool information. If the <i>poolname</i> argument is specified, only information on the specified pool is displayed. If the <i>poolname</i> argument is not specified, all pools are shown.</p> |
|-------------------------|--|

| | |
|-----------------|---|
| Examples | The following is sample output from the show ipv6 dhcp pool command: |
|-----------------|---|

```
Router# show ipv6 dhcp pool

DHCPv6 pool: svr-p1
Static bindings:
  Binding for client 000300010002FCA5C01C
    IA PD: IA ID 00040002,
      Prefix: 3FFE:C00:C18:3::/72
             preferred lifetime 604800, valid lifetime 2592000
    IA PD: IA ID not specified; being used by 00040001
      Prefix: 3FFE:C00:C18:1::/72
             preferred lifetime 240, valid lifetime 54321
      Prefix: 3FFE:C00:C18:2::/72
             preferred lifetime 300, valid lifetime 54333
      Prefix: 3FFE:C00:C18:3::/72
             preferred lifetime 280, valid lifetime 51111
Prefix from pool: local-p1, Valid lifetime 12345, Preferred lifetime 180
DNS server: 1001::1
DNS server: 1001::2
Domain name: domain1.net
Domain name: domain2.net
Domain name: domain3.net
Active clients: 2
```

Table 62 describes the significant fields shown in the display.

Table 62 *show ipv6 dhcp pool Field Descriptions*

| Field | Description |
|------------------------------------|--|
| DHCPv6 pool: svr-p1 | The name of the pool. |
| IAPD | Identity association for prefix delegation (IAPD), which is a collection of prefixes assigned to a client. |
| IAID | Identifier for this IAPD. |
| Prefix | Prefixes to be delegated to the indicated IAPD on the specified client. |
| preferred lifetime, valid lifetime | Lifetimes associated with the prefix statically assigned to the specified client. |
| DNS server | IPv6 addresses of the DNS servers. |
| Domain name | Displays the DNS domain search list. |
| Active clients | Total number of active clients. |

Related Commands

| Command | Description |
|-------------------------|---|
| ipv6 dhcp pool | Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode. |
| ipv6 dhcp server | Enables DHCP for IPv6 service on an interface. |

show ipv6 general-prefix

To display information on IPv6 general prefixes, use the **show ipv6 general-prefix** command in user EXEC or privileged EXEC mode.

show ipv6 general-prefix

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.3(4)T | This command was introduced. |

Usage Guidelines Use the **show ipv6 general-prefix** command to view information on IPv6 general prefixes.

Examples The following example shows an IPv6 general prefix called my-prefix, which has been defined based on a 6to4 interface. The general prefix is also being used to define an address on interface loopback42.

```
Router# show ipv6 general-prefix

IPv6 Prefix my-prefix, acquired via 6to4
2002:B0B:B0B::/48
  Loopback42 (Address command)
```

Table 63 describes the significant fields shown in the display.

Table 63 *show ipv6 general-prefix Field Descriptions*

| Field | Description |
|------------------------------|---|
| IPv6 Prefix | User-defined name of the IPv6 general prefix. |
| Acquired via | The general prefix has been defined based on a 6to4 interface. A general prefix can also be defined manually or acquired using DHCP for IPv6 prefix delegation. |
| 2002:B0B:B0B::/48 | The prefix value for this general prefix. |
| Loopback42 (Address command) | List of interfaces where this general prefix is used. |

| Related Commands | Command | Description |
|------------------|---------------------|--|
| | ipv6 general-prefix | Defines a general prefix for an IPv6 address manually. |

show ipv6 interface

To display the usability status of interfaces configured for IPv6, use the **show ipv6 interface** command in user EXEC or privileged EXEC mode.

```
show ipv6 interface [brief] [[interface-type interface-number] [prefix]]
```

| | | |
|--------------------|------------------|--|
| Syntax Description | brief | (Optional) Displays a brief summary of IPv6 status and configuration for each interface. |
| | interface-type | (Optional) Displays information about only this interface type. |
| | interface-number | (Optional) Displays information about only this interface number. |

Defaults Displays all IPv6 interfaces.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------|---|
| | 12.2(2)T | This command was introduced. |
| | 12.2(4)T | The OK, TENTATIVE, DUPLICATE, ICMP redirects, and ND DAD fields were added to the command output. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **show ipv6 interface** command provides output similar to the **show ip interface** command, except that it is IPv6-specific.

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable. A usable interface is one through which the software can send and receive packets. If the software determines that an interface is not usable, it removes the directly connected routing entry from the routing table. Removing the entry allows the software to use dynamic routing protocols to determine backup routes to the network (if any).

If the interface hardware is usable, the interface is marked “up.” If the interface can provide two-way communication, the line protocol is marked “up.”

If you specify an optional interface type and number, you will see information only about that specific interface.

Examples

Interface Information for a Specific Interface with IPv6 Configured

When you do not specify an interface type and number, information on all IPv6 interfaces is displayed. Specifying an interface type and number displays information about the specified interface. The following is sample output from the **show ipv6 interface** command when entered with an IPv6 interface type and number:

```
Router# show ipv6 interface ethernet 0

Ethernet0 is up, line protocol is up
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF11:6770
  MTU is 1500 bytes
  ICMP error messages limited to one every 500 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

Table 64 describes the significant fields shown in the display.

Table 64 *show ipv6 interface Field Descriptions*

| Field | Description |
|---|---|
| Ethernet 0 is up, down, administratively down (down and administratively down are not shown in sample output) | Indicates whether the interface hardware is currently active (whether line signal is present) and whether it has been taken down by an administrator. If the interface hardware is usable, the interface is marked “up.” For an interface to be usable, both the interface hardware and line protocol must be up. |
| line protocol is up, down (down is not shown in sample output) | Indicates whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful). If the interface can provide two-way communication, the line protocol is marked “up.” For an interface to be usable, both the interface hardware and line protocol must be up. |
| IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output) | Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked “enabled.” If duplicate address detection processing identified the link-local address of the interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked “stalled.” If IPv6 is not enabled, the interface is marked “disabled.” |
| link-local address | Displays the link-local address assigned to the interface. |

Table 64 *show ipv6 interface Field Descriptions (continued)*

| Field | Description |
|-----------------------------------|---|
| TENTATIVE | <p>The state of the address in relation to duplicate address detection. States can be any of the following:</p> <ul style="list-style-type: none"> • DUPLICATE—The address is not unique and is not being used. If the duplicate address is the link-local address of an interface, the processing of IPv6 packets is disabled on that interface. • OK—The address is unique and is being used. • TENTATIVE—Duplicate address detection is either pending or under way on this interface. <p>Note If an address does not have one of these states (the state for the address is blank), the address is unique and is being used.</p> |
| Global unicast address(es): | Displays the global unicast addresses assigned to the interface. |
| Joined group address(es): | Indicates the multicast groups to which this interface belongs. |
| MTU | Maximum transmission unit of the interface. |
| ICMP error messages | Specifies the minimum interval (in milliseconds) between error messages sent on this interface. |
| ICMP redirects | The state of Internet Control Message Protocol (ICMP) IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled). |
| ND DAD | The state of duplicate address detection on the interface (enabled or disabled). |
| number of DAD attempts: | Number of consecutive neighbor solicitation messages that are sent on the interface while duplicate address detection is performed. |
| ND reachable time | Displays the neighbor discovery reachable time (in milliseconds) assigned to this interface. |
| ND advertised reachable time | Displays the neighbor discovery reachable time (in milliseconds) that is advertised on this interface. |
| ND advertised retransmit interval | Displays the neighbor discovery retransmit interval (in milliseconds) that is advertised on this interface. |
| ND router advertisements | Specifies the interval (in seconds) for neighbor discovery router advertisements sent on this interface and the amount of time before the advertisements expire. |

show ipv6 interface Command Using the brief Keyword

The following is sample output from the **show ipv6 interface** command when entered with the **brief** keyword:

```
Router# show ipv6 interface brief

Ethernet0 is up, line protocol is up
Ethernet0                [up/up]
    unassigned
Ethernet1                  [up/up]
    2001:0DB8:1000:/29
```



```

Ethernet2                [up/up]
    2001:0DB8:2000:/29
Ethernet3                [up/up]
    2001:0DB8:3000:/29
Ethernet4                [up/down]
    2001:0DB8:4000:/29
Ethernet5                [administratively down/down]
    2001:123::210:7BFF:FEC2:ACD8

```

| Interface | Status | IPv6 Address |
|-----------|-----------------------|---------------------------------|
| Ethernet0 | up | 3FFE:C00:0:1:260:3EFF:FE11:6770 |
| Ethernet1 | up | unassigned |
| Fddi0 | up | 3FFE:C00:0:2:260:3EFF:FE11:6772 |
| Serial0 | administratively down | unassigned |
| Serial1 | administratively down | unassigned |
| Serial2 | administratively down | unassigned |
| Serial3 | administratively down | unassigned |
| Tunnel0 | up | unnumbered (Ethernet0) |
| Tunnel1 | up | 3FFE:700:20:1::12 |

IPv6 Interface with ND Prefix Configured

This example output shows the characteristics of an interface which has generated a prefix from a local IPv6 prefix pool.

```
Router# show ipv6 interface Virtual-Access 1.21 prefix
```

```

IPv6 Prefix Advertisements Virtual-Access1.21
Codes: A - Address, P - Prefix-Advertisement, O - Pool
X - Proxy RA, U - Per-user prefix, D - Default
N - Not advertised, C - Calendar

O 2001:0DB8::/29 [LA] Valid lifetime 2592000, preferred lifetime 604800

```

show ipv6 local pool

To display information about any defined IPv6 address pools, use the **show ipv6 local pool** command in privileged EXEC mode.

```
show ipv6 local pool [poolname [cache]]
```

| | | |
|--------------------|-----------------|---|
| Syntax Description | <i>poolname</i> | (Optional) User-defined name for the local address pool. |
| | cache | (Optional) Indicates that cache statistics are to be included in the output display |

| | |
|---------------|-----------------|
| Command Modes | Privileged EXEC |
|---------------|-----------------|

| | | |
|-----------------|-----------|------------------------------|
| Command History | Release | Modification |
| | 12.2(13)T | This command was introduced. |

| | |
|------------------|--|
| Usage Guidelines | If you omit the <i>poolname</i> argument, the command displays a generic list of all defined address pools and the IP addresses that belong to them. If you specify the <i>poolname</i> argument, the command displays detailed information about that pool. |
|------------------|--|

Examples The following command displays IPv6 prefix pool information, which includes cache statistics:

```
Router# show ipv6 local pool mypool

Prefix is 2001:0DB8::/29 assign /64 prefix
2 entries in use, 254 available, 0 rejected
0 entries cached, 1000 maximum

User          Prefix          Interface
joe           3FFE:FFFF:A::/64  Vi1
john          3FFE:FFFF:A:1::/64 Vi2
```

The following command displays IPv6 prefix pool information for all prefix pools:

```
Router# show ipv6 local pool

Pool Prefix Free In use
mypool 2001:0DB8::/29 65516 20
myrouter#
myrouter# show ipv6 local pool mypool
Prefix is 1234::/48 assign /64 prefix
20 entries in use, 65516 available, 0 rejected
0 entries cached, 1000 maximum
User Prefix Interface
user1-72b 1234::/64 Vi1.21
user1-72b 1234:0:0:1::/64 Vi1.22
user1-72b 1234:0:0:2::/64 Vi1.23
user1-72b 1234:0:0:3::/64 Vi1.24
user1-72b 1234:0:0:4::/64 Vi1.25
user1-72b 1234:0:0:5::/64 Vi1.26
```

```

user1-72b 1234:0:0:6::/64 Vi1.27
user1-72b 1234:0:0:7::/64 Vi1.28
user1-72b 1234:0:0:8::/64 Vi1.29
user1-72b 1234:0:0:9::/64 Vi1.30
user1-72b 1234:0:0:A::/64 Vi1.31
user1-72b 1234:0:0:B::/64 Vi1.32
user1-72b 1234:0:0:C::/64 Vi1.33
user1-72b 1234:0:0:D::/64 Vi1.34
user1-72b 1234:0:0:E::/64 Vi1.35
user1-72b 1234:0:0:F::/64 Vi1.36
user1-72b 1234:0:0:10::/64 Vi1.37
user1-72b 1234:0:0:11::/64 Vi1.38
user1-72b 1234:0:0:12::/64 Vi1.39
user1-72b 1234:0:0:13::/64 Vi1.40

```

Table 65 describes the significant fields shown in the displays.

Table 65 *show ipv6 local pool Field Descriptions*

| Field | Description |
|-------|--|
| Scope | The type of access. |
| Pool | Pool and group names and associations, if created. |
| Begin | The first IP address in the defined range of addresses in this pool. |
| End | The last IP address in the defined range of addresses in this pool. |
| Free | The number of addresses available. |
| InUse | The number of addresses in use. |

Related Commands

| Command | Description |
|------------------------|---|
| ipv6 local pool | Configures a local pool of IPv6 addresses to be used when a remote peer connects to a point-to-point interface. |

show ipv6 mfib

To display the forwarding entries and interfaces in the IPv6 Multicast Forwarding Information Base (MFIB), use the **show ipv6 mfib** command in user EXEC or privileged EXEC mode.

```
show ipv6 mfib [link-local | group-name | group-address [source-name | source-address]]
               [verbose]
```

| | | |
|--------------------|--|---|
| Syntax Description | link-local | (Optional) Displays the link-local groups. |
| | <i>group-name</i> <i>group-address</i> | (Optional) IPv6 address or name of the multicast group. |
| | <i>source-name</i> <i>source-address</i> | (Optional) IPv6 address or name of the multicast group. |
| | verbose | (Optional) Provides additional information, such as the MAC encapsulation header and platform-specific information. |
| | | |

Defaults No default behavior or values

Command Modes User EXEC
Privileged EXEC

| | | |
|-----------------|----------------|---|
| Command History | Release | Modification |
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | The link-local keyword was added. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines Use the **show ipv6 mfib** command to display MFIB entries, forwarding interfaces, and their traffic statistics. This command can be enabled on virtual IP (VIP) if the router is operating in distributed mode.

A forwarding entry in the MFIB has flags that determine the default forwarding and signaling behavior to use for packets matching the entry. The entry also has per-interface flags that further specify the forwarding behavior for packets received or forwarded on specific interfaces. Table 66 describes the MFIB forwarding entries and interface flags.

Table 66 MFIB Forwarding Entries and Interface Flags

| Flag | Description |
|------|--|
| F | Forward—Data is forwarded out of this interface. |
| A | Accept—Data received on this interface is accepted for forwarding. |
| IC | Internal copy—Deliver to the router a copy of the packets received or forwarded on this interface. |

Table 66 MFIB Forwarding Entries and Interface Flags (continued)

| Flag | Description |
|------|---|
| NS | Negate signal—Reverse the default entry signaling behavior for packets received on this interface. |
| DP | Do not preserve—When signaling the reception of a packet on this interface, do not preserve a copy of it (discard it instead). |
| SP | Signal present—The reception of a packet on this interface was just signaled. |
| S | Signal—By default, signal the reception of packets matching this entry. |
| C | Perform directly connected check for packets matching this entry. Signal the reception if packets were originated by a directly connected source. |

Examples

The following example displays the forwarding entries and interfaces in the MFIB. The router is configured for fast switching, and it has a receiver joined to FF05::1 on Ethernet1/1 and a source (2001::1:1:20) sending on Ethernet1/2:

```
Router# show ipv6 mfib

IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
              AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
                  IC - Internal Copy, NP - Not platform switched
                  SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,FF00::/8) Flags: C
  Forwarding: 0/0/0/0, Other: 0/0/0
  Tunnel0 Flags: NS
(*,FF00::/15) Flags: D
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF05::1) Flags: C
  Forwarding: 2/0/100/0, Other: 0/0/0
  Tunnel0 Flags: A NS
  Ethernet1/1 Flags: F NS
    Pkts: 0/2
(2001::1:1:200,FF05::1) Flags:
  Forwarding: 5/0/100/0, Other: 0/0/0
  Ethernet1/2 Flags: A
  Ethernet1/1 Flags: F NS
    Pkts: 3/2
(*,FF10::/15) Flags: D
  Forwarding: 0/0/0/0, Other: 0/0/0
```

Table 67 describes the significant fields shown in the display.

Table 67 show ipv6 mfib Field Descriptions

| Field | Description |
|-------------------|--|
| Entry flags | Information about the entry. |
| Forwarding Counts | Statistics on the packets that are received and forwarded to at least one interface. |
| Pkt Count/ | Total number of packets received and forwarded since the creation of the multicast forwarding state to which this counter applies. |

Table 67 *show ipv6 mfib Field Descriptions (continued)*

| Field | Description |
|-------------------|---|
| Pkts per second/ | Number of packets received and forwarded per second. |
| Avg Pkt Size/ | Total number of bytes divided by the total number of packets for this multicast forwarding state. There is no direct display for the total number of bytes. You can calculate the total number of bytes by multiplying the average packet size by the packet count. |
| Kbits per seco | Bytes per second divided by packets per second divided by 1000. |
| Other counts: | Statistics on the received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded. |
| Interface Flags: | Information about the interface. See Table 66 for further information on interface flags. |
| Interface Counts: | Interface statistics. |

show ipv6 mfib active

To display the rate at which active sources are sending to multicast groups, use the **show ipv6 mfib active** command in user EXEC or privileged EXEC mode.

show ipv6 mfib [**link-local** | *group-name* | *group-address*] **active** [*kbps*]

| | | |
|---------------------------|--|---|
| Syntax Description | link-local | (Optional) Displays the link-local groups. |
| | <i>group-name</i> <i>group-address</i> | (Optional) IPv6 address or name of the multicast group. |
| | <i>kbps</i> | (Optional) Kilobits per second. |
| | | |

| | |
|----------------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | The link-local keyword was added. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

| | |
|-------------------------|---|
| Usage Guidelines | Use the show ipv6 mfib active command to display MFIB entries actively used to forward packets. In many cases, it is useful to provide the optional <i>kbps</i> argument to limit the set of entries displayed to the ones that are forwarding an amount of traffic larger or equal to the amount set by the <i>kbps</i> argument. |
|-------------------------|---|

| | |
|-----------------|--|
| Examples | The following example displays statistics on the rate at which active IP multicast sources are sending information. The router is switching traffic from 2001::1:1:200 to FF05::1: |
|-----------------|--|

```
Router# show ipv6 mfib active
```

```
Active IPv6 Multicast Sources - sending >= 4 kbps
Group: FF05::1
  Source: 2001::1:1:200
    Rate: 20 pps/16 kbps(1sec), 0 kbps(last 128 sec)
```

Table 68 describes the significant fields shown in the display.

Table 68 *show ipv6 mfib active Field Descriptions*

| Field | Description |
|-------------|--|
| Group: | <p>Summary information about counters for (*, G) and the range of (S, G) states for one particular group G. The following RP-tree: and Source: output fields contain information about the individual states belonging to this group.</p> <p>Note For Source Specific Multicast (PIM-SSM) range groups, the Group: displays are statistical. All SSM range (S, G) states are individual, unrelated SSM channels.</p> |
| Rate...kbps | <p>Bytes per second divided by packets per second divided by 1000. On an IP multicast fast-switching platform, the number of packets per second is the number of packets during the last second. Other platforms may use a different approach to calculate this number. Please refer to the platform documentation for more information.</p> |

show ipv6 mfib count

To display summary traffic statistics from the Multicast Forwarding Information Base (MFIB) about the group and source, use the **show ipv6 mfib count** command in user EXEC or privileged EXEC mode.

show ipv6 mfib [**link-local** | *group-name* | *group-address* [*source-name* | *source-address*]] **count**

| Syntax Description | link-local | (Optional) Displays the link-local groups. |
|--------------------|--|---|
| | <i>group-name</i> <i>group-address</i> | (Optional) IPv6 address or name of the multicast group. |
| | <i>source-address</i> <i>source-name</i> | (Optional) Source address or name. |

| Command Modes | User EXEC Privileged EXEC |
|---------------|------------------------------|
|---------------|------------------------------|

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | The link-local keyword was added. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

| Usage Guidelines | The show ipv6 mfib count command also displays average packet size and data rate in kilobits per second. |
|------------------|---|
|------------------|---|

| Examples | The following example displays statistics from the MFIB about the group and source. The router is switching traffic from 2001::1:1:200 to FF05::1: |
|----------|--|
|----------|--|

```
Router# show ipv6 mfib count

IP Multicast Statistics
54 routes, 7 groups, 0.14 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group: FF00::/8
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
Group: FF00::/15
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
Group: FF05::1
  RP-tree: Forwarding: 2/0/100/0, Other: 0/0/0
  Source: 10::1:1:200, Forwarding: 367/10/100/7, Other: 0/0/0
  Tot. shown: Source count: 1, pkt count: 369
Group: FF10::/15
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
Group: FF20::/15
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
```

Table 69 describes the significant fields shown in the display.

Table 69 *show ipv6 mfib count Field Descriptions*

| Field | Description |
|--|--|
| Forwarding Counts | Statistics on the packets that are received and forwarded to at least one interface. |
| Pkt Count/ | Total number of packets received and forwarded since the multicast forwarding state to which this counter applies was created. |
| Pkts per second/ | Number of packets received and forwarded per second. |
| Avg Pkt Size/ | Total number of bytes divided by the total number of packets for this multicast forwarding state. There is no direct display for the total number of bytes. You can calculate the total number of bytes by multiplying the average packet size by the packet count. |
| Kilobits per second | Bytes per second divided by packets per second divided by 1000. |
| Other counts: | Statistics on the received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded. |
| Total/ | Total number of packets received. |
| RPF failed/ | Number of packets not forwarded due to a failed Reverse Path Forwarding (RPF) or acceptance check (when bidirectional PIM is configured). |
| Other drops (OIF-null, rate-limit etc) | Number of packets not forwarded for reasons other than an RPF or acceptance check (such as the outgoing interface [OIF] list was empty or because the packets were discarded because of a configuration that was enabled). |
| Group: | Summary information about counters for (*, G) and the range of (S, G) states for one particular group G. The following RP-tree: and Source: output fields contain information about the individual states belonging to this group. Note For Source Specific Multicast (PIM-SSM) range groups, the Group: displays are statistical. All SSM range (S, G) states are individual, unrelated SSM channels. |
| RP-tree: | Counters for the (*, G) state of this group G. These counters are displayed only for groups that have a forwarding mode that do not forward packets on the shared tree. These (*, G) groups are bidirectional PIM and PIM sparse mode (PIM-SM) groups. There are no RP-tree displays for PIM SSM range groups. |

show ipv6 mfib interface

To display information about IPv6 multicast-enabled interfaces and their forwarding status, use the **show ipv6 mfib interface** command in user EXEC or privileged EXEC mode.

show ipv6 mfib interface

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines The **show ipv6 mfib interface** command displays the Multicast Forwarding Information Base (MFIB) interfaces and in what switching mode each MFIB has been configured.

Examples The following example displays information about IPv6 multicast-enabled interfaces and their forwarding status. The router is configured for fast switching:

```
Router# show ipv6 mfib interface

IPv6 Multicast Forwarding (MFIB) status:
  Configuration Status: enabled
  Operational Status: running

MFIB interface      status      CEF-based output
                  [configured,available]
Ethernet1/1         up          [yes        ,yes      ]
Ethernet1/2         up          [yes        ,?        ]
Tunnel0             up          [yes        ,?        ]
Tunnel1            up          [yes        ,?        ]
```

Table 70 describes the significant fields shown in the display.

Table 70 show ipv6 mfib interface Field Descriptions

| Field | Description |
|------------------|---|
| MFIB interface | Specifies the MFIB interface. |
| Status | Specifies the status of the MFIB interface. |
| CEF-based output | Provides information on the CEF-based output of the MFIB interface. |

show ipv6 mfib status

To display the general Multicast Forwarding Information Base (MFIB) configuration and operational status, use the **show ipv6 mfib status** command in user EXEC or privileged EXEC mode.

show ipv6 mfib status

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|-----------|--|
| 12.0(26)S | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

show ipv6 mfib summary

To display summary information about the number of IPv6 Multicast Forwarding Information Base (MFIB) entries (including link-local groups) and interfaces, use the **show ipv6 mfib summary** command in user EXEC or privileged EXEC mode.

show ipv6 mfib summary

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines The **show ipv6 mfib summary** command shows the IP multicast routing table in abbreviated form. The command displays only the number of MFIB entries, the number of (*, G) and (S, G) entries, and the number of MFIB interfaces specified.

The **show ipv6 mfib summary** command counts all entries, including link-local entries.

Examples The following example displays summary information about the number of IPv6 MFIB entries and interfaces:

```
Router# show ipv6 mfib summary

IPv6 MFIB summary:
  54      total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]
  17      total MFIB interfaces
```

Table 71 describes the significant fields shown in the display.

Table 71 *show ipv6 mfib summary* Field Descriptions

| Field | Description |
|--------------------------|--|
| 54 total entries | Total number of MFIB entries, including the number of (*, G) and (S, G) entries. |
| 17 total MFIB interfaces | Sum of all the MFIB interfaces in all the MFIB entries. |

show ipv6 mld groups

To display the multicast groups that are directly connected to the router and that were learned through Multicast Listener Discovery (MLD), use the **show ipv6 mld groups** command in user EXEC or privileged EXEC mode.

```
show ipv6 mld groups [link-local] [group-name | group-address] [interface-type
                        interface-number] [detail]
```

Syntax Description

| | |
|--|--|
| <i>group-name group-address</i> | (Optional) IPv6 address or name of the multicast group. |
| link-local | (Optional) Displays the link-local groups. |
| <i>interface-type interface-number</i> | (Optional) Interface type and number. |
| detail | (Optional) Displays detailed information about individual sources. |

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.3(2)T | This command was introduced. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| 12.0(26)S | The link-local keyword was added. |
| 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines

If you omit all optional arguments, the **show ipv6 mld groups** command displays by group address and interface type and number all directly connected multicast groups, including link-local groups (where the **link-local** keyword is not available) used.

Examples

The following is sample output from the **show ipv6 mld groups** command. It shows all of the groups joined by Fast Ethernet interface 2/1, including link-local groups used by network protocols.

```
Router# show ipv6 mld groups FastEthernet 2/1

MLD Connected Group Membership
Group Address      Interface      Uptime      Expires
FF02::2            FastEthernet2/1 3d18h      never
FF02::D            FastEthernet2/1 3d18h      never
FF02::16           FastEthernet2/1 3d18h      never
FF02::1:FF00:1     FastEthernet2/1 3d18h      00:00:27
FF02::1:FF00:79    FastEthernet2/1 3d18h      never
FF02::1:FF23:83C2  FastEthernet2/1 3d18h      00:00:22
FF02::1:FFAF:2C39  FastEthernet2/1 3d18h      never
FF06:7777::1       FastEthernet2/1 3d18h      00:00:26
```

The following is sample output from the **show ipv6 mld groups** command using the **detail** keyword:

```
Router# show ipv6 mld groups detail

Interface:      Ethernet0
Group:          FF17::1
Uptime:         00:52:31
Router mode:    EXCLUDE (Expires:never)
Host mode:      EXCLUDE
Last reporter:  FE80::208:20FF:FE08:D7FF
Source list is empty
Interface:      POS1/0
Group:          FF05::21:9
Uptime:         00:26:44
Router mode:    EXCLUDE (Expires:never)
Host mode:      EXCLUDE
Last reporter:  FE80::208:20FF:FE08:D554
Source list is empty
```

Table 72 describes the significant fields shown in the display.

Table 72 *show ipv6 mld groups Field Descriptions*

| Field | Description |
|----------------|---|
| Group Address | Address of the multicast group. |
| Interface | Interface through which the group is reachable. |
| Uptime | How long (in hours, minutes, and seconds) this multicast group has been known. |
| Expires | How long (in hours, minutes, and seconds) until the entry is removed from the MLD groups table. The expiration timer shows “never” if the router itself has joined the group, and the expiration timer shows “not used” when the router mode of the group is INCLUDE. In this situation, the expiration timers on the source entries are used. |
| Last reporter: | Last host to report being a member of the multicast group. |

Related Commands

| Command | Description |
|--------------------------------|---|
| ipv6 mld query-interval | Configures the frequency at which the Cisco IOS software sends MLD host-query messages. |

show ipv6 mld groups summary

To display the number of (*, G) and (S, G) membership reports present in the Multicast Listener Discovery (MLD) cache, use the **show ipv6 mld groups summary** command in user EXEC or privileged EXEC mode..

show ipv6 mld groups summary

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines The **show ipv6 mld groups summary** command displays the number of directly connected multicast groups (including link-local groups).

Examples The following is sample output from the **show ipv6 mld groups summary** command:

```
Router# show ipv6 mld groups summary
```

```
MLD Route Summary
  No. of (*,G) routes = 5
  No. of (S,G) routes = 0
```

Table 73 describes the significant fields shown in the display.

Table 73 *show ipv6 mld groups summary Field Descriptions*

| Field | Description |
|-------------------------|---|
| No. of (*,G) routes = 5 | Displays the number of groups present in the MLD cache. |
| No. of (S,G) routes = 0 | Displays the number of include and exclude mode sources present in the MLD cache. |

show ipv6 mld interface

To display multicast-related information about an interface, use the **show ipv6 mld interface** command in user EXEC or privileged EXEC mode.

show ipv6 mld interface [*type number*]

| | |
|---------------------------|--|
| Syntax Description | <i>type number</i> (Optional) Interface type and number. |
|---------------------------|--|

| | |
|----------------------|------------------------------|
| Command Modes | User EXEC Privileged EXEC |
|----------------------|------------------------------|

| Command History | Release | Modification |
|------------------------|-----------|---|
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

| | |
|-------------------------|---|
| Usage Guidelines | If you omit the optional <i>type</i> and <i>number</i> arguments, the show ipv6 mld interface command displays information about all interfaces. |
|-------------------------|---|

| | |
|-----------------|---|
| Examples | The following is sample output from the show ipv6 mld interface command for Fast Ethernet interface 2/1: |
|-----------------|---|

```
Router# show ipv6 mld interface FastEthernet 2/1

FastEthernet2/1 is up, line protocol is up
Internet address is FE80::205:5FFF:FEAF:2C39/10
MLD is enabled in interface
Current MLD version is 2
MLD query interval is 125 seconds
MLD querier timeout is 255 seconds
MLD max query response time is 10 seconds
Last member query response interval is 1 seconds
MLD activity: 25 joins, 17 leaves
MLD querying router is FE80::205:5FFF:FEAF:2C39 (this system)
```

Table 74 describes the significant fields shown in the display.

Table 74 *show ipv6 mld interface Field Descriptions*

| Field | Description |
|--|---|
| FastEthernet2/1 is up, line protocol is up | Interface type, number, and status. |
| Internet address is... | Internet address of the interface and subnet mask being applied to the interface. |

Table 74 *show ipv6 mld interface Field Descriptions (continued)*

| Field | Description |
|---|--|
| MLD is enabled in interface | Indicates whether Multicast Listener Discovery (MLD) has been enabled on the interface with the ipv6 multicast-routing command. |
| Current MLD version is 2 | The current MLD version. |
| MLD query interval is 125 seconds | Interval (in seconds) at which the Cisco IOS software sends MLD query messages, as specified with the ipv6 mld query-interval command. |
| MLD querier timeout is 255 seconds | The length of time (in seconds) before the router takes over as the querier for the interface, as specified with the ipv6 mld query-timeout command. |
| MLD max query response time is 10 seconds | The length of time (in seconds) that hosts have to answer an MLD Query message before the router deletes their group, as specified with the ipv6 mld query-max-response-time command. |
| Last member query response interval is 1 seconds | Used to calculate the maximum response code inserted in group and source-specific query. Also used to tune the “leave latency” of the link. A lower value results in reduced time to detect the last member leaving the group. |
| MLD activity: 25 joins, 17 leaves | Number of groups joins and leaves that have been received. |
| MLD querying router is FE80::205:5FFF:FEAF:2C39 (this system) | IPv6 address of the querying router. |

Related Commands

| Command | Description |
|--------------------------------|---|
| ipv6 mld join-group | Configures MLD reporting for a specified group and source. |
| ipv6 mld query-interval | Configures the frequency at which the Cisco IOS software sends MLD host-query messages. |

show ipv6 mld traffic

To display the Multicast Listener Discovery (MLD) traffic counters, use the **show ipv6 mld traffic** command in user EXEC or privileged EXEC mode.

show ipv6 mld traffic

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|--|
| | 12.0(26)S | This command was introduced. |
| | 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines Use the **show ipv6 mld traffic** command to check if the expected number of MLD protocol messages have been received and sent.

Examples The following example displays the MLD protocol messages received and sent.

```
Router# show ipv6 mld traffic

MLD Traffic Counters
Elapsed time since counters cleared:00:00:21

Valid MLD Packets          Received    Sent
Queries                    1           0
Reports                    2           1
Leaves                     0           0
Mtrace packets             0           0

Errors:
Malformed Packets          0
Bad Checksums              0
Martian source             0
Packets Received on MLD-disabled Interface 0
```

Table 75 describes the significant fields shown in the display.

Table 75 *show ipv6 mld traffic Field Descriptions*

| Field | Description |
|-------------------------------------|---|
| Elapsed time since counters cleared | Indicates the amount of time (in hours, minutes, and seconds) since the counters cleared. |
| Valid MLD packets | Number of valid MLD packets received and sent. |

Table 75 *show ipv6 mld traffic Field Descriptions (continued)*

| Field | Description |
|----------------|--|
| Queries | Number of valid queries received and sent. |
| Reports | Number of valid reports received and sent. |
| Leaves | Number of valid leaves received and sent. |
| Mtrace packets | Number of multicast trace packets received and sent. |
| Errors | Types of errors and the number of errors that have occurred. |

show ipv6 mrib client

To display information about the clients of the Multicast Routing Information Base (MRIB), use the **show ipv6 mrib client** command in user EXEC or privileged EXEC mode.

show ipv6 mrib client [**filter**] [**name** {*client-name* | *client-name:client-id*}]

| | | |
|---------------------------|------------------------------|---|
| Syntax Description | filter | (Optional) Displays information about MRIB flags that each client owns and that each client is interested in. |
| | name | (Optional) The name of a multicast routing protocol that acts as a client of MRIB, such as Multicast Listener Discovery (MLD) and Protocol Independent Multicast (PIM). |
| | <i>client-name:client-id</i> | The name and ID of a multicast routing protocol that acts as a client of MRIB, such as MLD and PIM. The colon is required. |

| | |
|----------------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

| | |
|-------------------------|--|
| Usage Guidelines | Use the filter keyword to display information about the MRIB flags each client owns and the flags in which each client is interested. |
|-------------------------|--|

Examples The following is sample output from the **show ipv6 mrib client** command:

```
Router# show ipv6 mrib client

IP MRIB client-connections
igmp:145          (connection id 0)
pim:146 (connection id 1)
mfib ipv6:3      (connection id 2)
slot 3  mfib ipv6 rp agent:16  (connection id 3)
slot 1  mfib ipv6 rp agent:16  (connection id 4)
slot 0  mfib ipv6 rp agent:16  (connection id 5)
slot 4  mfib ipv6 rp agent:16  (connection id 6)
slot 2  mfib ipv6 rp agent:16  (connection id 7)
```

Table 76 describes the significant fields shown in the display.

Table 76 *show ipv6 mrib client Field Descriptions*

| Field | Description |
|--|------------------------------------|
| igmp:145 (connection id 0) pim:146 (connection id 1) mfib ipv6:3 (connection id 2) mfib ipv6 rp agent:16 (connection id 3) | Client ID (client name:process ID) |

show ipv6 mrib route

To display the Multicast Routing Information Base (MRIB) route information, use the **show ipv6 mrib route** command in user EXEC or privileged EXEC mode.

```
show ipv6 mrib route [link-local | summary | source-address | source-name | *] [group-name | group-address [prefix-length]]
```

| | | |
|---------------------------|--|--|
| Syntax Description | link-local | (Optional) Displays the link-local groups. |
| | summary | (Optional) Displays the number of MRIB entries (including link-local groups) and interfaces present in the MRIB table. |
| | <i>source-address</i> <i>source-name</i> | (Optional) IPv6 address or name of the source. |
| | * | (Optional) Displays all MRIB route information. |
| | <i>group-name</i> <i>group-address</i> | (Optional) IPv6 address or name of the multicast group. |
| | <i>prefix-length</i> | (Optional) IPv6 prefix length. |

| | |
|----------------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | The link-local keyword was added. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines

All entries are created by various clients of MRIB, such as Multicast Listener Discovery (MLD), Protocol Independent Multicast (PIM), and Multicast Forwarding Information Base (MFIB). The flags on each entry or interface serve as a communication mechanism between various clients of MRIB. The entries reveal how PIM sends register messages for new sources and the action taken.

The **summary** keyword shows the count of all entries, including link-local entries.

The interface flags are described in Table 77.

Table 77 Description of Interface Flags

| Flag | Description |
|------|---|
| F | Forward—Data is forwarded out of this interface |
| A | Accept—Data received on this interface is accepted for forwarding |
| IC | Internal copy |
| NS | Negate signal |

Table 77 Description of Interface Flags

| Flag | Description |
|------|----------------------------------|
| DP | Do not preserve |
| SP | Signal present |
| II | Internal interest |
| ID | Internal uninterest |
| LI | Local interest |
| LD | Local uninterest |
| C | Perform directly connected check |

Special entries in the MRIB indicate exceptions from the normal behavior. For example, no signaling or notification is necessary for arriving data packets that match any of the special group ranges. The special group ranges are as follows:

- Undefined scope (FFX0::/16)
- Node local groups (FFX1::/16)
- Link-local groups (FFX2::/16)
- Source Specific Multicast (SSM) groups (FF3X::/32).

For all the remaining (usually sparse-mode) IPv6 multicast groups, directly connected check is performed and the PIM notified if a directly connected source arrives. This procedure is how PIM sends register messages for new sources.

Examples

The following is sample output from the **show ipv6 mrib route** command using the **summary** keyword:

```
Router# show ipv6 mrib route summary

MRIB Route-DB Summary
  No. of (*,G) routes = 52
  No. of (S,G) routes = 0
  No. of Route x Interfaces (RxI) = 10
```

Table 78 describes the significant fields shown in the display.

Table 78 show ipv6 mrib route Field Descriptions

| Field | Description |
|---------------------------------|---|
| No. of (*, G) routes | Number of shared tree routes in the MRIB. |
| No. of (S, G) routes | Number of source tree routes in the MRIB. |
| No. of Route x Interfaces (RxI) | Sum of all the interfaces on each MRIB route entry. |
| RPF nbr | IP address of the upstream router to the RP or source. |
| Flags | Information set by the MRIB clients on this MRIB entry. |
| Tunnel5 flags and POS flags | Information set by the MRIB clients on this MRIB interface. |

show ipv6 mroute

To display the information in the PIM topology table in a format similar to the **show ip mroute** command, use the **show ipv6 mroute** command in user EXEC or privileged EXEC mode.

```
show ipv6 mroute [link-local | [group-name | group-address [source-address | source-name]]
[summary] [count]
```

| | | |
|---------------------------|--|--|
| Syntax Description | link-local | (Optional) Displays the link-local groups. |
| | <i>group-name</i> <i>group-address</i> | (Optional) IPv6 address or name of the multicast group. |
| | <i>source-address</i> <i>source-name</i> | (Optional) IPv6 address or name of the source. |
| | summary | (Optional) Displays a one-line, abbreviated summary of each entry in the IPv6 multicast routing table. |
| | count | (Optional) Displays statistics from the Multicast Forwarding Information Base (MFIB) about the group and source, including number of packets, packets per second, average packet size, and bytes per second. |
| | | |

Defaults The **show ipv6 mroute** command displays all groups and sources.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|------------------------|----------------|---|
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | The link-local keyword was added. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines The IPv6 multicast implementation does not have a separate mroute table. For this reason, the **show ipv6 mroute** command enables you to display the information in the PIM topology table in a format similar to the **show ip mroute** command.

If you omit all optional arguments and keywords, the **show ipv6 mroute** command displays all the entries in the PIM topology table (except link-local groups where the **link-local** keyword is available).

The Cisco IOS software populates the PIM topology table by creating (S,G) and (*,G) entries based on PIM protocol messages, MLD reports, and traffic. The asterisk (*) refers to all source addresses, the “S” refers to a single source address, and the “G” is the destination multicast group address. In creating (S, G) entries, the software uses the best path to that destination group found in the unicast routing table (that is, through Reverse Path Forwarding [RPF]).

Use the **show ipv6 mrib** command to display the forwarding status of each IPv6 multicast route.

Examples

The following is sample output from the **show ipv6 mroute** command:

```
Router# show ipv6 mroute ff07::1

Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
      C - Connected, L - Local, I - Received Source Specific Host Report,
      P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
      J - Join SPT
Timers:Uptime/Expires
Interface state:Interface, State

(*, FF07::1), 00:04:45/00:02:47, RP 2001:0DB8:6::6, flags:S
  Incoming interface:Tunnel5
  RPF nbr:6:6:6::6
  Outgoing interface list:
    POS4/0, Forward, 00:04:45/00:02:47

(2001:0DB8:999::99, FF07::1), 00:02:06/00:01:23, flags:SFT
  Incoming interface:POS1/0
  RPF nbr:2001:0DB8:999::99
  Outgoing interface list:
    POS4/0, Forward, 00:02:06/00:03:27
```

The following is sample output from the **show ipv6 mroute** command with the **summary** keyword:

```
Router# show ipv6 mroute ff07::1 summary

Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
      C - Connected, L - Local, I - Received Source Specific Host Report,
      P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
      J - Join SPT
Timers:Uptime/Expires
Interface state:Interface, State

(*, FF07::1), 00:04:55/00:02:36, RP 2001:0DB8:6::6, OIF count:1, flags:S

(2001:0DB8:999::99, FF07::1), 00:02:17/00:01:12, OIF count:1, flags:SFT
```

The following is sample output from the **show ipv6 mroute** command with the **count** keyword:

```
Router# show ipv6 mroute ff07::1 count

IP Multicast Statistics
71 routes, 24 groups, 0.04 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group:FF07::1
  RP-tree:
    RP Forwarding:0/0/0/0, Other:0/0/0
    LC Forwarding:0/0/0/0, Other:0/0/0
  Source:2001:0DB8:999::99,
    RP Forwarding:0/0/0/0, Other:0/0/0
    LC Forwarding:0/0/0/0, Other:0/0/0
    HW Forwd: 20000/0/92/0, Other:0/0/0
  Tot. shown:Source count:1, pkt count:20000
```

Table 79 describes the significant fields shown in the display.

Table 79 *show ipv6 mroute Field Descriptions*

| Field | Description |
|------------------------|---|
| Flags: | <p>Provides information about the entry.</p> <ul style="list-style-type: none"> • S—sparse. Entry is operating in sparse mode. • s—SSM group. Indicates that a multicast group is within the SSM range of IP addresses. This flag is reset if the SSM range changes. • C—connected. A member of the multicast group is present on the directly connected interface. • L—local. The router itself is a member of the multicast group. • I—received source specific host report. Indicates that an (S, G) entry was created by an (S, G) report. This flag is set only on the designated router (DR). • P—pruned. Route has been pruned. The Cisco IOS software keeps this information so that a downstream member can join the source. • R—RP-bit set. Indicates that the (S, G) entry is pointing toward the RP. This is typically prune state along the shared tree for a particular source. • F—register flag. Indicates that the software is registering for a multicast source. • T—SPT-bit set. Indicates that packets have been received on the shortest path source tree. |
| | <ul style="list-style-type: none"> • J—join SPT. For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold value set for the group. (The default SPT-Threshold setting is 0 kbps.) When the J - Join shortest path tree (SPT) flag is set, the next (S, G) packet received down the shared tree triggers an (S, G) join in the direction of the source, thereby causing the router to join the source tree. <p>The default SPT-Threshold value of 0 kbps is used for the group, and the J - Join SPT flag is always set on (*, G) entries and is never cleared. The router immediately switches to the shortest path source tree when traffic from a new source is received.</p> |
| Timers: Uptime/Expires | <p>“Uptime” indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IPv6 multicast routing table.</p> <p>“Expires” indicates per interface how long (in hours, minutes, and seconds) until the entry will be removed from the IPv6 multicast routing table.</p> |

Table 79 *show ipv6 mroute Field Descriptions (continued)*

| Field | Description |
|--------------------------------------|--|
| Interface state: | <p>Indicates the state of the incoming or outgoing interface.</p> <ul style="list-style-type: none"> Interface. Indicates the type and number of the interface listed in the incoming or outgoing interface list. Next-Hop. “Next-Hop” specifies the IP address of the downstream neighbor. State/Mode. “State” indicates that packets will either be forwarded, pruned, or null on the interface depending on whether there are restrictions due to access lists. “Mode” indicates that the interface is operating in sparse mode. |
| (*, FF07::1) and (2001:0DB8:999::99) | <p>Entry in the IPv6 multicast routing table. The entry consists of the IPv6 address of the source router followed by the IPv6 address of the multicast group. An asterisk (*) in place of the source router indicates all sources.</p> <p>Entries in the first format are referred to as (*, G) or “star comma G” entries. Entries in the second format are referred to as (S, G) or “S comma G” entries; (*, G) entries are used to build (S, G) entries.</p> |
| RP | Address of the RP router. |
| flags: | Information set by the MRIB clients on this MRIB entry. |
| Incoming interface: | Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded. |
| RPF nbr | IP address of the upstream router to the RP or source. |
| Outgoing interface list: | Interfaces through which packets will be forwarded. For (S,G) entries, this list will not include the interfaces inherited from the (*,G) entry. |

Related Commands

| Command | Description |
|-------------------------------|--|
| ipv6 multicast-routing | Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding. |
| show ipv6 mfib | Displays the forwarding entries and interfaces in the IPv6 MFIB. |

show ipv6 mroute active

To display the active multicast streams on the router, use the **show ipv6 mroute active** command in user EXEC or privileged EXEC mode.

show ipv6 mroute [**link-local** | *group-name* | *group-address*] **active** [*kbps*]

| | | |
|---------------------------|--|--|
| Syntax Description | link-local | (Optional) Displays the link-local groups. |
| | <i>group-name</i> <i>group-address</i> | (Optional) IPv6 address or name of the multicast group. |
| | <i>kbps</i> | (Optional) Displays the rate that active sources are sending to multicast groups. Active sources are those sending at the kbps value or higher. The <i>kbps</i> argument defaults to 4 kbps. |
| | | |

Defaults The *kbps* argument defaults to 4 kbps.

Command Modes User EXEC
Privileged EXEC

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | The link-local keyword was added. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines The **show ipv6 mroute active** command displays active multicast streams with data rates that are greater than or equal to the kilobits per second set by the user. The command default is 4 kbps.

Examples The following is sample output from the **show ipv6 mroute active** command:

```
Router# show ipv6 mroute active

Active IPv6 Multicast Sources - sending >= 4 kbps
Group:FF05::1
  Source:2001::1:1:1
    Rate:11 pps/8 kbps(1sec), 8 kbps(last 8 sec)
```

Table 80 describes the significant fields shown in the display.

Table 80 *show ipv6 mroute active Field Descriptions*

| Field | Description |
|-------------|--|
| Group: | <p>Summary information about counters for (*, G) and the range of (S, G) states for one particular group G. The following RP-tree: and Source: output fields contain information about the individual states belonging to this group.</p> <p>Note For Source Specific Multicast (PIM-SSM) range groups, the Group: displays are statistical. All SSM range (S, G) states are individual, unrelated SSM channels.</p> |
| Rate...kbps | <p>Bytes per second divided by packets per second divided by 1000. On an IP multicast fast-switching platform, the number of packets per second is the number of packets during the last second. Other platforms may use a different approach to calculate this number. Please refer to the platform documentation for more information.</p> |

show ipv6 mtu

To display maximum transmission unit (MTU) cache information for IPv6 interfaces, use the **show ipv6 mtu** command in user EXEC or privileged EXEC mode.

show ipv6 mtu

Syntax Description This command has no keywords or arguments

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Examples The following is sample output from the **show ipv6 mtu** command:

```
Router# show ipv6 mtu

MTU      Since      Destination Address
1400     00:04:21   5000:1::3
1280     00:04:50   FE80::203:A0FF:FED6:141D
```

Table 81 describes the significant fields shown in the display.

Table 81 *show ipv6 mtu Field Descriptions*

| Field | Description |
|---------------------|---|
| MTU | MTU, which was contained in the Internet Control Message Protocol (ICMP) packet-too-big message, used for the path to the destination address. |
| Since | Age of the entry since the ICMP packet-too-big message was received. |
| Destination Address | Address contained in the received ICMP packet-too-big message. Packets originating from this router to this address should be no bigger than the given MTU. |

| Related Commands | Command | Description |
|------------------|----------|---|
| | ipv6 mtu | Sets the MTU size of IPv6 packets sent on an interface. |

show ipv6 nat statistics

To display Network Address Translation - Protocol Translation (NAT-PT) statistics, use the **show iv6 nat statistics** command in user EXEC or privileged EXEC mode.

show ipv6 nat statistics

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 12.2(13)T | This command was introduced. |

Examples The following is sample output from the **show ipv6 nat statistics** command:

```
Router# show ipv6 nat statistics
```

```
Total active translations: 4 (2 static, 2 dynamic; 2 extended)
NAT-PT interfaces:
  Ethernet3/1, Ethernet3/3
Hits: 1 Misses: 1
Expired translations: 0
```

Table 82 describes the significant fields shown in the display.

Table 82 *show ipv6 nat statistics Field Descriptions*

| Field | Description |
|---------------------------|--|
| Total active translations | Number of translations active in the system. This number increments by one each time a translation is created and is decremented each time a translation is cleared or times out. Displays the numbers for each type of translation. |
| NAT-PT interfaces | The interfaces, by type and number, that are configured to run NAT-PT translations. |
| Hits | Number of times the software does a translations table lookup and finds an entry. |
| Misses | Number of times the software does a translations table lookup, fails to find an entry, and must try to create one. |
| Expired translations | Cumulative count of translations that have expired since the router was booted. |

| Related Commands | Command | Description |
|------------------|-----------------------------------|--------------------------------------|
| | show ipv6 nat translations | Displays active NAT-PT translations. |

show ipv6 nat translations

To display active Network Address Translation - Protocol Translation (NAT-PT) translations, use the **show ip nat translations** command in user EXEC or privileged EXEC mode.

show ipv6 nat translations [icmp | tcp | udp] [verbose]

| | | |
|---------------------------|----------------|---|
| Syntax Description | icmp | (Optional) Displays detailed information about NAT-PT ICMP translation events. |
| | tcp | (Optional) Displays detailed information about NAT-PT TCP translation events. |
| | udp | (Optional) Displays detailed information about NAT-PT User Datagram Protocol (UDP) translation events. |
| | verbose | (Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used. |

| | |
|----------------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 12.2(13)T | This command was introduced. |

Examples The following is sample output from the **show ip nat translations** command. Two static translations have been configured between an IPv4 source address and an IPv6 destination, and vice versa.

Router# **show ipv6 nat translations**

```

Prot  IPv4 source          IPv6 source
     IPv4 destination  IPv6 destination
---  ---              ---
     192.168.123.2      2001::2

---  ---              ---
     192.168.122.10     2001::10

tcp   192.168.124.8,11047  3002::8,11047
     192.168.123.2,23   2001::2,23

udp   192.168.124.8,52922  3002::8,52922
     192.168.123.2,69   2001::2,69

udp   192.168.124.8,52922  3002::8,52922
     192.168.123.2,52922 2001::2,52922

---   192.168.124.8      3002::8
     192.168.123.2      2001::2

---   192.168.124.8      3002::8
     ---                ---

---   192.168.121.4      5001::4

```

The following is sample output that includes the **verbose** keyword:

```
Router# show ipv6 nat translations verbose

Prot  IPv4 source          IPv6 source
      IPv4 destination  IPv6 destination
---   ---
      192.168.123.2      2001::2
      create 00:04:24, use 00:03:24,

---   ---
      192.168.122.10     2001::10
      create 00:04:24, use 00:04:24,

tcp    192.168.124.8,11047  3002::8,11047
      192.168.123.2,23    2001::2,23
      create 00:03:24, use 00:03:20, left 00:16:39,

udp    192.168.124.8,52922  3002::8,52922
      192.168.123.2,69    2001::2,69
      create 00:02:51, use 00:02:37, left 00:17:22,

udp    192.168.124.8,52922  3002::8,52922
      192.168.123.2,52922 2001::2,52922
      create 00:02:48, use 00:02:30, left 00:17:29,

---    192.168.124.8      3002::8
      192.168.123.2      2001::2
      create 00:03:24, use 00:02:34, left 00:17:25,

---    192.168.124.8      3002::8
      ---
      create 00:04:24, use 00:03:24,

---    192.168.121.4      5001::4
      ---
      create 00:04:25, use 00:04:25,
```

Table 83 describes the significant fields shown in the display.

Table 83 *show ipv6 nat translations Field Descriptions*

| Field | Description |
|-----------------------------------|--|
| Prot | Protocol of the port identifying the address. |
| IPv4 source/IPv6 source | The IPv4 or IPv6 source address to be translated. |
| IPv4 destination/IPv6 destination | The IPv4 or IPv6 destination address. |
| create | How long ago the entry was created (in hours:minutes:seconds). |
| use | How long ago the entry was last used (in hours:minutes:seconds). |
| left | Time before the entry times out (in hours:minutes:seconds). |

Related Commands

| Command | Description |
|-----------------------------------|--|
| clear ipv6 nat translation | Clears dynamic NAT-PT translations from the translation state table. |

show ipv6 neighbors

To display IPv6 neighbor discovery cache information, use the **show ipv6 neighbors** command in user EXEC or privileged EXEC mode.

show ipv6 neighbors [*interface-type interface-number* | *ipv6-address* | *ipv6-hostname*]

| | | |
|---------------------------|-------------------------|--|
| Syntax Description | <i>interface-type</i> | (Optional) Specifies the type of the interface from which IPv6 neighbor information is to be displayed. |
| | <i>interface-number</i> | (Optional) Specifies the number of the interface from which IPv6 neighbor information is to be displayed. |
| | <i>ipv6-address</i> | (Optional) Specifies the IPv6 address of the neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| | <i>ipv6-hostname</i> | (Optional) Specifies the IPv6 host name of the remote networking device. |

Defaults All IPv6 neighbor discovery cache information is displayed.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|------------------------|----------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.2(8)T | Support for static entries in the IPv6 neighbor discovery cache was added to the command output. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines When the *interface-type* and *interface-number* arguments are not specified, cache information for all IPv6 neighbors is displayed. Specifying the *interface-type* and *interface-number* arguments displays only cache information about the specified interface.

Examples The following is sample output from the **show ipv6 neighbors** command when entered with an interface type and number:

```
Router# show ipv6 neighbors ethernet 2
```

| IPv6 Address | Age | Link-layer Addr | State | Interface |
|--------------------------|-----|-----------------|-------|-----------|
| 2000:0:0:4::2 | 0 | 0003.a0d6.141e | REACH | Ethernet2 |
| FE80::203:A0FF:FED6:141E | 0 | 0003.a0d6.141e | REACH | Ethernet2 |
| 3001:1::45a | - | 0002.7d1a.9472 | REACH | Ethernet2 |

The following is sample output from the **show ipv6 neighbors** command when entered with an IPv6 address:

```
Router# show ipv6 neighbors 2000:0:0:4::2
```

| IPv6 Address | Age | Link-layer Addr | State | Interface |
|---------------|-----|-----------------|-------|-----------|
| 2000:0:0:4::2 | 0 | 0003.a0d6.141e | REACH | Ethernet2 |

Table 84 describes the significant fields shown in the displays.

Table 84 *show ipv6 neighbors Field Descriptions*

| Field | Description |
|-----------------|---|
| IPv6 Address | IPv6 address of neighbor or interface. |
| Age | Time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry. |
| Link-layer Addr | MAC address. If the address is unknown, a hyphen (-) is displayed. |

Table 84 show ipv6 neighbors Field Descriptions (continued)

| Field | Description |
|-----------|---|
| State | <p>The state of the neighbor cache entry. Following are the states for dynamic entries in the IPv6 neighbor discovery cache:</p> <ul style="list-style-type: none"> • INCMP (Incomplete)—Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received. • REACH (Reachable)—Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent. • STALE—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent. • DELAY—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE. • PROBE—A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received. • ???—Unknown state. <p>Following are the possible states for static entries in the IPv6 neighbor discovery cache:</p> <ul style="list-style-type: none"> • INCMP (Incomplete)—The interface for this entry is down. • REACH (Reachable)—The interface for this entry is up. <p>Note Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP (Incomplete) and REACH (Reachable) states are different for dynamic and static cache entries.</p> |
| Interface | Interface from which the address was reachable. |

show ipv6 ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the **show ipv6 ospf** command in user EXEC or privileged EXEC mode.

```
show ipv6 ospf [process-id] [area-id]
```

| | | |
|--------------------|------------|--|
| Syntax Description | process-id | (Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled. |
| | area-id | (Optional) Displays only information about a specified area. |

| | |
|---------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.3(4)T | Command output is changed when authentication is enabled. |

Examples The following is sample output from the **show ipv6 ospf** command:

```
Router# show ipv6 ospf

Routing Process "ospfv3 1" with ID 10.10.10.1
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Area BACKBONE(0)
    Number of interfaces in this area is 1
    MD5 Authentication, SPI 1000
    SPF algorithm executed 2 times
    Number of LSA 5. Checksum Sum 0x02A005
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

Table 85 describes the significant fields shown in the display.

Table 85 *show ipv6 ospf Field Descriptions*

| Field | Description |
|---|---|
| Routing process “ospfv3 1” with ID 172.16.3.3 | Process ID and OSPF router ID. |
| LSA group pacing timer | Configured LSA group pacing timer (in seconds). |
| Interface flood pacing timer | Configured LSA flood pacing timer (in milliseconds). |
| Retransmission pacing timer | Configured LSA retransmission pacing timer (in milliseconds). |
| Number of areas | Number of areas in router, area addresses, and so on. |

show ipv6 ospf border-routers

To display the internal OSPF routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the **show ipv6 ospf border-routers** command in user EXEC or privileged EXEC mode.

show ip ospf [*process-id*] **border-routers**

| | | |
|---------------------------|-------------------|--|
| Syntax Description | <i>process-id</i> | (Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled. |
|---------------------------|-------------------|--|

| | |
|----------------------|------------------------------|
| Command Modes | User EXEC Privileged EXEC |
|----------------------|------------------------------|

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Examples The following is sample output from the **show ip ospf border-routers** command:

```
Router# show ipv6 ospf border-routers
```

```
OSPFv3 Process 1 internal Routing Table
```

```
Codes: i - Intra-area route, I - Inter-area route
```

```
i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

Table 86 describes the significant fields shown in the display.

Table 86 *show ipv6 ospf border-routers Field Descriptions*

| Field | Description |
|--|--|
| i - Intra-area route, I - Inter-area route | The type of this route. |
| 172.16.4.4, 172.16.3.3 | Router ID of the destination router. |
| [2], [1] | Metric used to reach the destination router. |
| FE80::205:5FFF:FED3:5808, FE80::205:5FFF:FED3:5406, FE80::205:5FFF:FED3:5808 | Link-local routers. |
| FastEthernet0/0, POS4/0 | The interface on which the IPv6 OSPF protocol is configured. |

Table 86 *show ipv6 ospf border-routers Field Descriptions (continued)*

| Field | Description |
|----------------------|--|
| ABR | Area border router. |
| ASBR | Autonomous system boundary router. |
| Area 0, Area 1 | The area ID of the area from which this route is learned. |
| SPF 13, SPF 8, SPF 3 | The internal number of the shortest path first (SPF) calculation that installs this route. |

show ipv6 ospf database

To display lists of information related to the OSPF database for a specific router, use the **show ipv6 ospf database** command in EXEC mode. The various forms of this command deliver information about different OSPF link-state advertisements (LSAs).

```
show ipv6 ospf [process-id] [area-id] database
```

```
show ipv6 ospf [process-id] [area-id] database [adv-router [router-id]]
```

```
show ipv6 ospf [process-id] [area-id] database [database-summary]
```

```
show ipv6 ospf [process-id] [area-id] database [external [link-state-id] [adv-router | internal |  
self-originate ] [ipv6-address]]
```

```
show ipv6 ospf [process-id] [area-id] database [inter-area prefix [link-state-id] [adv-router |  
internal | self-originate ] | [ipv6-address]]
```

```
show ipv6 ospf [process-id] [area-id] database [inter-area router [link-state-id] [adv-router |  
internal | self-originate ] | [destination-router-id]]
```

```
show ipv6 ospf [process-id] [area-id] database [link] [link-state-id] [adv-router | internal |  
self-originate ] [interface [interface-name]]
```

```
show ipv6 ospf [process-id] [area-id] database [network] [link-state-id] [adv-router | internal |  
self-originate ]
```

```
show ipv6 ospf [process-id] [area-id] database [nssa-external [link-state-id] [adv-router |  
internal | self-originate ] | [ipv6-address]]
```

```
show ipv6 ospf [process-id] [area-id] database [prefix] [link-state-id] [adv-router | internal |  
self-originate ] [ref-lsa {router | network}]
```

```
show ipv6 ospf [process-id] [area-id] database [router] [adv-router | internal | self-originate ]  
[link-state-id]
```

```
show ipv6 ospf [process-id] [area-id] database [self-originate] [link-state-id]
```

Syntax Description

| | |
|-------------------|---|
| <i>process-id</i> | (Optional) Displays information only about a specified process. |
| <i>area-id</i> | (Optional) Displays information only about a specified area. |

| | |
|---|--|
| adv-router [<i>router-id</i>] | (Optional) Displays all the LSAs of the specified router. This argument must be in the form documented in RFC 2740 where the address is specified in hexadecimal using 16-bit values between colons. |
| 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. |
| <i>link-state-id</i> | (Optional) An integer used to differentiate LSAs. In network and link LSAs, the link-state ID matches the interface index. |
| internal | (Optional) Internal LSA information. |
| self-originate | (Optional) Displays only self-originated LSAs (from the local router). |
| <i>ipv6-address</i> | (Optional) Link-local IPv6 address of the neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| <i>destination-router-id</i> | (Optional) The specified destination router ID. |
| inter-area prefix | (Optional) Displays information only about LSAs based on inter-area prefix LSAs. |
| inter-area router | (Optional) Displays information only about LSAs based on inter-area router LSAs. |
| link | (Optional) Displays information about the link LSAs. |
| interface | (Optional) Displays information about the LSAs filtered by interface context. |
| <i>interface-name</i> | (Optional) Specifies the LSA interface. |
| 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 on the intra-area-prefix LSAs. |
| ref-lsa { router network } | (Optional) Further filters the prefix LSA type. |
| router | (Optional) Displays information only about the router LSAs. |

Command Modes EXEC

| Command History | Release | Modification |
|------------------------|----------------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines The **adv-router** keyword requires a router ID. The **self-originate** keyword displays only those LSAs that originated from the local router. Both of these keywords can be appended to all other keywords used with the **show ipv6 ospf** database command to provide more detailed information.

Examples

The following is sample output from the **show ipv6 ospf database** command when no arguments or keywords are used:

```
Router# show ipv6 ospf database

        OSPFv3 Router with ID (172.16.4.4) (Process ID 1)

        Router Link States (Area 0)

ADV Router      Age      Seq#      Fragment ID  Link count  Bits
172.16.4.4      239      0x80000003  0            1           B
172.16.6.6      239      0x80000003  0            1           B

        Inter Area Prefix Link States (Area 0)

ADV Router      Age      Seq#      Prefix
172.16.4.4      249      0x80000001  FEC0:3344::/32
172.16.4.4      219      0x80000001  FEC0:3366::/32
172.16.6.6      247      0x80000001  FEC0:3366::/32
172.16.6.6      193      0x80000001  FEC0:3344::/32
172.16.6.6      82       0x80000001  FEC0::/32

        Inter Area Router Link States (Area 0)

ADV Router      Age      Seq#      Link ID      Dest RtrID
172.16.4.4      219      0x80000001  50529027     172.16.3.3
172.16.6.6      193      0x80000001  50529027     172.16.3.3

        Link (Type-8) Link States (Area 0)

ADV Router      Age      Seq#      Link ID      Interface
172.16.4.4      242      0x80000002  14           PO4/0
172.16.6.6      252      0x80000002  14           PO4/0

        Intra Area Prefix Link States (Area 0)

ADV Router      Age      Seq#      Link ID      Ref-lstype  Ref-LSID
172.16.4.4      242      0x80000002  0            0x2001      0
172.16.6.6      252      0x80000002  0            0x2001      0
```

Table 87 describes the significant fields shown in the display.

Table 87 show ipv6 ospf database Field Descriptions

| Field | Description |
|------------|---|
| ADV Router | Advertising router ID. |
| Age | Link-state age. |
| Seq# | Link-state sequence number (detects old or duplicate LSAs). |
| Link ID | Interface ID number. |
| Ref-lstype | Referenced link-state type. |
| Ref-LSID | Referenced link-state ID. |

The following is sample output from the **show ipv6 ospf database** command with the **router self-originate** keywords:

```
Router# show ipv6 ospf database router self-originate

        OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
```

```

Router Link States (Area 0)

LS age: 383
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Router Links
Link State ID: 0
Advertising Router: 172.16.6.6
LS Seq Number: 80000003
Checksum: 0x7543
Length: 40
Area Border Router
Number of Links: 1

Link connected to: another Router (point-to-point)
Link Metric: 1
Local Interface ID: 14
Neighbor Interface ID: 14
Neighbor Router ID: 172.16.4.4

```

The following is sample output from the **show ipv6 ospf database** command with the **network** keyword:

```

Router# show ipv6 ospf database network

OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

Net Link States (Area 1)

LS age: 419
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Network Links
Link State ID: 3 (Interface ID of Designated Router)
Advertising Router: 172.16.6.6
LS Seq Number: 80000001
Checksum: 0x8148
Length: 32
    Attached Router: 172.16.6.6
    Attached Router: 172.16.3.3

```

The following is sample output from the **show ipv6 ospf database** command with the **link self-originate** keywords:

```

Router# show ipv6 ospf database link self-originate

OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

Link (Type-8) Link States (Area 0)

LS age: 505
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Link-LSA (Interface: POS4/0)
Link State ID: 14 (Interface ID)
Advertising Router: 172.16.6.6
LS Seq Number: 80000002
Checksum: 0xABF6
Length: 60
Router Priority: 1
Link Local Address: FE80::205:5FFF:FED3:6408
Number of Prefixes: 2
Prefix Address: FEC0:4466::
Prefix Length: 32, Options: None
Prefix Address: FEC0:4466::
Prefix Length: 32, Options: None

```

The following is sample output from the **show ipv6 ospf database** command with the **prefix self-originate** keywords:

```
Router# show ipv6 ospf database prefix self-originate

      OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

      Intra Area Prefix Link States (Area 0)

Routing Bit Set on this LSA
LS age: 552
LS Type: Intra-Area-Prefix-LSA
Link State ID: 0
Advertising Router: 172.16.6.6
LS Seq Number: 80000002
Checksum: 0xA910
Length: 48
Referenced LSA Type: 2001
Referenced Link State ID: 0
Referenced Advertising Router: 172.16.6.6
Number of Prefixes: 2
Prefix Address: FEC0:4466::
Prefix Length: 32, Options: None, Metric: 1
Prefix Address: FEC0:4466::
Prefix Length: 32, Options: None, Metric: 1
```

The following is sample output from the **show ipv6 ospf database** command with the **inter-area prefix self-originate** keywords:

```
Router# show ipv6 ospf database inter-area prefix self-originate

      OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

      Inter Area Prefix Link States (Area 0)

LS age: 587
LS Type: Inter Area Prefix Links
Link State ID: 0
Advertising Router: 172.16.6.6
LS Seq Number: 80000001
Checksum: 0x1395
Length: 32
Metric: 1
Prefix Address: FEC0:3366::
Prefix Length: 32, Options: None

LS age: 532
LS Type: Inter Area Prefix Links
Link State ID: 1
Advertising Router: 172.16.6.6
LS Seq Number: 80000001
Checksum: 0x3197
Length: 32
Metric: 2
Prefix Address: FEC0:3344::
Prefix Length: 32, Options: None

LS age: 422
LS Type: Inter Area Prefix Links
Link State ID: 2
Advertising Router: 172.16.6.6
LS Seq Number: 80000001
Checksum: 0xCB74
Length: 32
```

```

Metric: 1
Prefix Address: FEC0::
Prefix Length: 32, Options: None

```

The following is sample output from the **show ipv6 ospf database** command with the **inter-area router self-originate** keywords:

```

Router# show ipv6 ospf database inter-area router self-originate

      OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

      Inter Area Router Link States (Area 0)

LS age: 578
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Inter Area Router Links
Link State ID: 50529027
Advertising Router: 172.16.6.6
LS Seq Number: 80000001
Checksum: 0x369F
Length: 32
Metric: 1
Destination Router ID: 172.16.3.3

```

The following is sample output from the **show ipv6 ospf database** command with the **external** keyword:

```

Router# show ipv6 ospf database external

      OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

      Type-5 AS External Link States

Routing Bit Set on this LSA
LS age: 654
LS Type: AS External Link
Link State ID: 0
Advertising Router: 172.16.3.3
LS Seq Number: 80000001
Checksum: 0x218D
Length: 32
Prefix Address: FEC0:3333::
Prefix Length: 32, Options: None
Metric Type: 2 (Larger than any link state path)
Metric: 20

```

show ipv6 ospf flood-list

To display a list of OSPF link-state advertisements (LSAs) waiting to be flooded over an interface, use the **show ipv6 ospf flood-list** command in EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] **flood-list** *interface-type interface-number*

Syntax Description

| | |
|-------------------------|--|
| <i>process-id</i> | (Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled. |
| <i>area-id</i> | (Optional) Displays information only about a specified area. |
| interface-type | Interface type over which the LSAs will be flooded. |
| interface-number | Interface number over which the LSAs will be flooded. |

Command Modes

EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.0(24)S | This command was introduced. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines

Use this command to display OSPF packet pacing.

Examples

The following is sample output from the **show ipv6 ospf flood-list** command:

```
Router# show ipv6 ospf flood-list
```

```
OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
```

```
Interface POS4/0, Queue length 1
Link state retransmission due in 14 msec
```

| Type | LS ID | ADV RTR | Seq NO | Age | Checksum |
|--------|-------|------------|------------|-----|----------|
| 0x2001 | 0 | 172.16.6.6 | 0x80000031 | 0 | 0x1971 |

```
Interface FastEthernet0/0, Queue length 0
```

```
Interface ATM3/0, Queue length 0
```


Table 88 describes the significant fields shown in the display.

Table 88 *show ipv6 ospf flood-list Field Descriptions*

| Field | Description |
|---|--|
| OSPFv3 Router with ID (172.16.6.6) (Process ID 1) | Identification of the router for which information is displayed. |
| Interface POS4/0 | 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. |

show ipv6 ospf interface

To display Open Shortest Path First (OSPF)-related interface information, use the **show ipv6 ospf interface** command in user EXEC or privileged mode.

show ipv6 ospf [*process-id*] [*area-id*] **interface** [*interface-type interface-number*]

| | | |
|---------------------------|-------------------------|--|
| Syntax Description | <i>process-id</i> | (Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled. |
| | <i>area-id</i> | (Optional) Displays only information about a specified area. |
| | <i>interface-type</i> | (Optional) Interface type and number. |
| | <i>interface-number</i> | |

| | |
|----------------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| Command History | Release | Modification |
|------------------------|-----------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.3(4)T | Command output is changed when authentication is enabled. |

Examples The following is sample output from the **show ipv6 ospf interface** command:

```
Router# show ipv6 ospf interface

ATM3/0 is up, line protocol is up
  Link Local Address FE80::205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address FE80::205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address FE80::205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address FE80::205:5FFF:FED3:5808
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```

Hello due in 00:00:05
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 12, maximum is 12
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 172.16.6.6  (Designated Router)
Suppress hello for 0 neighbor(s)

```

Table 89 describes the significant fields shown in the display.

Table 89 *show ipv6 ospf interface Field Descriptions*

| Field | Description |
|---|---|
| ATM3/0 | Status of the physical link and operational status of protocol. |
| Link Local Address | Interface IPv6 address. |
| Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3 | The area ID, process ID, instance ID, and router ID of the area from which this route is learned. |
| Network Type POINT_TO_POINT, Cost: 1 | 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. |
| Hello | Number of seconds until the next hello packet is sent out this interface. |
| Neighbor Count | Count of network neighbors and list of adjacent neighbors. |

The following is sample output from the **show ipv6 ospf interface** command with authentication enabled using interface configuration:

```

Router# show ipv6 ospf interface

Ethernet0/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication SPI 500, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 11.11.11.1, local address FE80::A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
FE80::A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 11.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)

```

The following is sample output from the **show ipv6 ospf interface** command with null authentication configured on the interface:

```
Router# show ipv6 ospf interface

Ethernet0/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  Authentication NULL
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 11.11.11.1, local address FE80::A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
FE80::A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 11.11.11.1 (Designated Router)
  Suppress hello for 0 neighbor(s)
```

The following is sample output from the **show ipv6 ospf interface** command with authentication configured for the area:

```
Router# show ipv6 ospf interface

Ethernet0/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication (Area) SPI 1000, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 11.11.11.1, local address FE80::A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
FE80::A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 11.11.11.1 (Designated Router)
  Suppress hello for 0 neighbor(s)
```

show ipv6 ospf neighbor

To display OSPF neighbor information on a per-interface basis, use the **show ipv6 ospf neighbor** command in EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] **neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**]

| | | |
|---------------------------|--|--|
| Syntax Description | <i>process-id</i> | (Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled. |
| | <i>area-id</i> | (Optional) Displays information only about a specified area. |
| | <i>interface-type</i> <i>interface-number</i> | (Optional) Interface type and number. |
| | <i>neighbor-id</i> | (Optional) Neighbor ID. |
| | detail | (Optional) Displays all neighbors in detail (lists all neighbors). |

| | |
|----------------------|------|
| Command Modes | EXEC |
|----------------------|------|

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Examples

The following is sample output from the **show ipv6 ospf neighbor** command:

```
Router# show ipv6 ospf neighbor
```

| Neighbor ID | Pri | State | Dead Time | Interface ID | Interface |
|-------------|-----|----------|-----------|--------------|----------------|
| 172.16.4.4 | 1 | FULL/ - | 00:00:31 | 14 | POS4/0 |
| 172.16.3.3 | 1 | FULL/BDR | 00:00:30 | 3 | FastEthernet00 |
| 172.16.5.5 | 1 | FULL/ - | 00:00:33 | 13 | ATM3/0 |

The following is sample output from the **show ipv6 ospf neighbor** command with the **detail** keyword:

```
Router# show ipv6 ospf neighbor detail
```

```
Neighbor 172.16.4.4
  In the area 0 via interface POS4/0
  Neighbor: interface-id 14, link-local address FE80::205:5FFF:FED3:5406
  Neighbor priority is 1, State is FULL, 6 state changes
  Options is 0x63AD1B0D
  Dead timer due in 00:00:33
  Neighbor is up for 00:48:56
  Index 1/1/1, retransmission queue length 0, number of retransmission 1
  First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec
Neighbor 172.16.3.3
```

```

In the area 1 via interface FastEthernet0/0
Neighbor: interface-id 3, link-local address FE80::205:5FFF:FED3:5808
Neighbor priority is 1, State is FULL, 6 state changes
DR is 172.16.6.6 BDR is 172.16.3.3
Options is 0x63F813E9
Dead timer due in 00:00:33
Neighbor is up for 00:09:00
Index 1/1/2, retransmission queue length 0, number of retransmission 2
First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
Last retransmission scan length is 1, maximum is 2
Last retransmission scan time is 0 msec, maximum is 0 msec
Neighbor 172.16.5.5
In the area 2 via interface ATM3/0
Neighbor: interface-id 13, link-local address FE80::205:5FFF:FED3:6006
Neighbor priority is 1, State is FULL, 6 state changes
Options is 0x63F7D249
Dead timer due in 00:00:38
Neighbor is up for 00:10:01
Index 1/1/3, retransmission queue length 0, number of retransmission 0
First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
Last retransmission scan length is 0, maximum is 0
Last retransmission scan time is 0 msec, maximum is 0 msec

```

Table 90 describes the significant fields shown in the display.

Table 90 *show ipv6 ospf neighbor Field Descriptions*

| Field | Description |
|---------------------------------|---|
| Neighbor ID; Neighbor | Neighbor router ID. |
| In the area | Area and interface through which the OSPF neighbor is known. |
| Pri; Neighbor priority | Router priority of the neighbor, neighbor state. |
| State | OSPF state. |
| State changes | Number of state changes since the neighbor was created. |
| 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 due in | Expected time before Cisco IOS software will declare the neighbor dead. |
| Neighbor is up for | Number of hours:minutes:seconds since the neighbor went into two-way state. |
| Index | Neighbor location in the area-wide and autonomous system-wide retransmission queue. |
| retransmission queue length | Number of elements in the retransmission queue. |
| number of retransmission | Number of times update packets have been re-sent during flooding. |
| First | Memory location of the flooding details. |
| Next | Memory location of the flooding details. |
| Last retransmission scan length | Number of link state advertisements (LSAs) in the last retransmission packet. |

Table 90 *show ipv6 ospf neighbor Field Descriptions (continued)*

| Field | Description |
|-------------------------------|---|
| maximum | Maximum number of LSAs sent in any retransmission packet. |
| Last retransmission scan time | Time taken to build last retransmission packet. |
| maximum | Maximum time taken to build any retransmission packet. |

show ipv6 ospf request-list

To display a list of all link-state advertisements (LSAs) requested by a router, use the **show ipv6 ospf request-list** command in EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

| | |
|---------------------------|--|
| <i>process-id</i> | (Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled. |
| <i>area-id</i> | (Optional) Displays information only about a specified area. |
| <i>neighbor</i> | (Optional) Displays the list of all LSAs requested by the router from this neighbor. |
| <i>interface</i> | (Optional) Displays the list of all LSAs requested by the router from this interface. |
| <i>interface-neighbor</i> | (Optional) Displays the list of all LSAs requested by the router on this interface, from this neighbor. |

Command Modes

EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.0(24)S | This command was introduced. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines

The information displayed by the **show ipv6 ospf request-list** command is useful in debugging OSPF routing operations.

Examples

The following example shows information about the LSAs requested by the router:

```
Router# show ipv6 ospf request-list
```

```
OSPFv3 Router with ID (192.168.255.5) (Process ID 1)
```

```
Neighbor 192.168.255.2, interface Ethernet0/0 address  
FE80::A8BB:CCFF:FE00:6600
```

| Type | LS ID | ADV RTR | Seq NO | Age | Checksum |
|------|---------|---------------|------------|-----|----------|
| 1 | 0.0.0.0 | 192.168.255.3 | 0x800000C2 | 1 | 0x0014C5 |
| 1 | 0.0.0.0 | 192.168.255.2 | 0x800000C8 | 0 | 0x000BCA |
| 1 | 0.0.0.0 | 192.168.255.1 | 0x800000C5 | 1 | 0x008CD1 |
| 2 | 0.0.0.3 | 192.168.255.3 | 0x800000A9 | 774 | 0x0058C0 |
| 2 | 0.0.0.2 | 192.168.255.3 | 0x800000B7 | 1 | 0x003A63 |

Table 91 describes the significant fields shown in the display.

Table 91 *show ipv6 ospf request-list Field Descriptions*

| Field | Description |
|---|--|
| OSPFv3 Router with ID (192.168.255.5) (Process ID 1) | Identification of the router for which information is displayed. |
| Interface Ethernet0/0 | Interface for which information is displayed. |
| 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. |

show ipv6 ospf retransmission-list

To display a list of all link-state advertisements (LSAs) waiting to be re-sent, use the **show ipv6 ospf retransmission-list** command in EXEC mode.

```
show ipv6 ospf [process-id] [area-id] retransmission-list [neighbor] [interface]
[interface-neighbor]
```

Syntax Description

| | |
|---------------------------|--|
| <i>process-id</i> | (Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled. |
| <i>area-id</i> | (Optional) Displays information only about a specified area. |
| <i>neighbor</i> | (Optional) Displays the list of all LSAs waiting to be re-sent for this neighbor. |
| <i>interface</i> | (Optional) Displays the list of all LSAs waiting to be re-sent on this interface. |
| <i>interface-neighbor</i> | (Optional) Displays the list of all LSAs waiting to be re-sent on this interface, from this neighbor. |

Command Modes

EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.0(24)S | This command was introduced. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines

The information displayed by the **show ipv6 ospf retransmission-list** command is useful in debugging OSPF routing operations.

Examples

The following is sample output from the **show ipv6 ospf retransmission-list** command:

```
Router# show ipv6 ospf retransmission-list
```

```
OSPFv3 Router with ID (192.168.255.2) (Process ID 1)
```

```
Neighbor 192.168.255.1, interface Ethernet0/0
```

```
Link state retransmission due in 3759 msec, Queue length 1
```

| Type | LS ID | ADV RTR | Seq NO | Age | Checksum |
|--------|-------|---------------|------------|-----|----------|
| 0x2001 | 0 | 192.168.255.2 | 0x80000222 | 1 | 0x00AE52 |

Table 92 describes the significant fields shown in the display.

Table 92 *show ipv6 ospf retransmission-list Field Descriptions*

| Field | Description |
|---|--|
| OSPFv3 Router with ID (192.168.255.2) (Process ID 1) | Identification of the router for which information is displayed. |
| Interface Ethernet0/0 | Interface for which information is displayed. |
| Link state retransmission due in | Length of time before next link-state transmission. |
| Queue length | Number of elements in the retransmission queue. |
| 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. |

show ipv6 ospf summary-prefix

To display a list of all summary address redistribution information configured under an OSPF process, use the **show ipv6 ospf summary-prefix** command in EXEC mode.

show ipv6 ospf [*process-id*] **summary-prefix**

| | | |
|--------------------|-------------------|--|
| Syntax Description | <i>process-id</i> | (Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled. |
|--------------------|-------------------|--|

| | |
|---------------|------|
| Command Modes | EXEC |
|---------------|------|

| | | |
|-----------------|-----------|---|
| Command History | Release | Modification |
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

| | |
|------------------|---|
| Usage Guidelines | The <i>process-id</i> argument can be entered as a decimal number or as an IPv6 address format. |
|------------------|---|

Examples

The following is sample output from the **show ipv6 ospf summary-prefix** command:

```
Router# show ipv6 ospf summary-prefix

OSPFv3 Process 1, Summary-prefix

FEC0::/24 Metric 16777215, Type 0, Tag 0
```

Table 93 describes the significant fields shown in the display.

Table 93 *show ipv6 ospf summary-prefix* Field Descriptions

| Field | Description |
|----------------|--|
| OSPFv3 Process | Process ID of the router for which information is displayed. |
| Metric | Metric used to reach the destination router. |
| Type | Type of link-state advertisement (LSA). |
| Tag | LSA tag. |

show ipv6 ospf virtual-links

To display parameters and the current state of OSPF virtual links, use the **show ipv6 ospf virtual-links** command in EXEC mode.

show ipv6 ospf virtual-links

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines The information displayed by the **show ipv6 ospf virtual-links** command is useful in debugging OSPF routing operations.

Examples The following is sample output from the **show ipv6 ospf virtual-links** command:

```
Router# show ipv6 ospf virtual-links

Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```

Table 94 describes the significant fields shown in the display.

Table 94 *show ipv6 ospf virtual-links Field Descriptions*

| Field | Description |
|---|--|
| Virtual Link to router 172.16.6.6 is up | Specifies the OSPF neighbor, and if the link to that neighbor is up or down. |
| Interface ID | Interface ID and IPv6 address of the router. |
| Transit area 2 | The transit area through which the virtual link is formed. |
| via interface ATM3/0 | The interface through which the virtual link is formed. |

Table 94 *show ipv6 ospf virtual-links Field Descriptions (continued)*

| Field | Description |
|-------------------------|--|
| Cost of using 1 | The cost of reaching the OSPF neighbor through the virtual link. |
| Transmit Delay is 1 sec | The transmit delay (in seconds) on the virtual link. |
| State POINT_TO_POINT | The state of the OSPF neighbor. |
| Timer intervals... | The various timer intervals configured for the link. |
| Hello due in 0:00:06 | When the next hello is expected from the neighbor. |

show ipv6 pim bsr

To display information about all bootstrap routers (BSRs) from which bootstrap messages (BSMs) have occurred in the last 130 seconds, use the **show ipv6 pim bsr** command in user EXEC or privileged EXEC mode.

show ipv6 pim bsr

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

| | |
|-----------------|-------------------------------|
| Defaults | No default behavior or values |
|-----------------|-------------------------------|

| | |
|----------------------|------------------------------|
| Command Modes | User EXEC Privileged EXEC |
|----------------------|------------------------------|

| | | |
|------------------------|----------------|--|
| Command History | Release | Modification |
| | 12.0(26)S | This command was introduced. |
| | 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

| | |
|-------------------------|---|
| Usage Guidelines | Use the show ipv6 pim bsr command to check if the router has received and forwarded any BSMs. The command displays information about the BSR address, Reverse Path Forwarding (RPF) information, priority, uptime, and expiration. |
|-------------------------|---|

A Cisco IOS IPv6 router will not disrupt the flow of BSMs. The router will recognize and parse enough of the BSM to identify the BSR address. It will do an RPF check for this BSR address and forward the packet only if it is received on the RPF interface. The router also creates a BSR entry containing RPF information to use for future BSMs from the same BSR. When BSMs from a given BSR are no longer received, the BSR entry is timed out.

| | |
|-----------------|---|
| Examples | The following example display information about all BSRs from which BSM messages have occurred in the last 130 seconds: |
|-----------------|---|

```
Router# show ipv6 pim bsr

PIMv2 BSR information
  BSR Address:2001::1:1:10
  Uptime:00:00:18, BSR Priority:255, Hash mask length:126
  RPF:2001::1:1:10,Ethernet2/0
  Expires:00:01:51
```

show ipv6 pim group-map

To display an IPv6 multicast group mapping table, use the **show ipv6 pim group-map** command in privileged EXEC mode.

```
show ipv6 pim group-map [group-name | group-address]
```

| | | |
|--------------------|----------------------------|---|
| Syntax Description | group-name group-address | (Optional) IPv6 address or name of the multicast group. |
|--------------------|----------------------------|---|

| | |
|---------------|-----------------|
| Command Modes | Privileged EXEC |
|---------------|-----------------|

| | | |
|-----------------|-----------|---|
| Command History | Release | Modification |
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

| | |
|------------------|--|
| Usage Guidelines | The show ipv6 pim group-map command displays group-to-mode mapping and rendezvous point (RP) information in sparse mode groups. |
|------------------|--|

| | |
|----------|---|
| Examples | The following is sample output from the show ipv6 pim group-map command: |
|----------|---|

```
Router# show ipv6 pim group-map

FF33::/32*
  RP      :::
  Protocol:SSM
  Client  :config
  Groups  :0
  Info    :
.
.
.
FF34::/32*
  RP      :::
  Protocol:SSM
  Client  :config
  Groups  :0
  Info    :
```

Table 95 describes the significant fields shown in the display.

Table 95 *show ipv6 pim group-map Field Descriptions*

| Field | Description |
|----------|--|
| RP | Address of the RP router if the protocol is sparse mode. |
| Protocol | <p>Protocol used: sparse mode (SM), Source Specific Multicast (SSM), link-local (LL), or NOROUTE (NO).</p> <p>LL is used for the link-local scoped IPv6 address range (ff[0-f]2::/16). LL is treated as a separate protocol type, because packets received with these destination addresses are not forwarded, but the router might need to receive and process them.</p> <p>NOROUTE or NO is used for the reserved and node-local scoped IPv6 address range (ff[0-f][0-1]::/16). These addresses are nonroutable, and the router does not need to process them.</p> |
| Client | Client from where mapping was learned. |
| Groups | How many groups are present in the topology table from this range. |
| Info | Reverse path forwarding (RPF) information from the RP. |

show ipv6 pim interface

To display information about interfaces configured for Protocol Independent Multicast (PIM), use the **show ipv6 pim interface** command in privileged EXEC mode.

```
show ipv6 pim interface [state-on] [state-off] [type number]
```

| | | |
|--------------------|--------------------|---|
| Syntax Description | state-on | (Optional) Displays interfaces with PIM enabled. |
| | state-off | (Optional) Displays interfaces with PIM disabled. |
| | <i>type number</i> | (Optional) Interface type and number. |

| | |
|---------------|-----------------|
| Command Modes | Privileged EXEC |
|---------------|-----------------|

| | | |
|-----------------|----------------|---|
| Command History | Release | Modification |
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | The state-on and state-off keywords were added. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines The **show ipv6 pim interface** command is used to check if PIM is enabled on an interface, the number of neighbors, and the designated router (DR) on the interface.

Examples The following is sample output from the **show ipv6 pim interface** command using the **state-on** keyword:

```
Router# show ipv6 pim interface state-on

Interface          PIM  Nbr   Hello  DR
                   Count Intvl Prior

Ethernet0          on   0     30     1
  Address:FE80::208:20FF:FE08:D7FF
  DR      :this system
POS1/0             on   0     30     1
  Address:FE80::208:20FF:FE08:D554
  DR      :this system
POS4/0             on   1     30     1
  Address:FE80::208:20FF:FE08:D554
  DR      :FE80::250:E2FF:FE8B:4C80
POS4/1             on   0     30     1
  Address:FE80::208:20FF:FE08:D554
  DR      :this system
Loopback0          on   0     30     1
  Address:FE80::208:20FF:FE08:D554
  DR      :this system
```

Table 96 describes the significant fields shown in the display.

Table 96 *show ipv6 pim interface Field Descriptions*

| Field | Description |
|-------------|---|
| Interface | Interface type and number that is configured to run PIM. |
| PIM | Whether PIM is enabled on an interface. |
| Nbr Count | Number of PIM neighbors that have been discovered through this interface. |
| Hello Intvl | Frequency, in seconds, of PIM hello messages. |
| DR | IP address of the designated router (DR) on a network. |
| Address | Interface IP address of the next-hop router. |

Related Commands

| Command | Description |
|-------------------------------|--|
| show ipv6 pim neighbor | Displays the PIM neighbors discovered by the Cisco IOS software. |

show ipv6 pim join-prune statistic

To display the average join-prune aggregation for the most recently aggregated 1000, 10,000, and 50,000 packets for each interface, use the **show ipv6 pim join-prune statistic** command in user EXEC or privileged EXEC mode.

```
show ipv6 pim join-prune statistic [interface-type]
```

| | | |
|--------------------|----------------|--|
| Syntax Description | interface-type | (Optional) Interface type. For more information, use the question mark (?) online help function. |
|--------------------|----------------|--|

| | |
|---------------|------------------------------|
| Command Modes | User EXEC Privileged EXEC |
|---------------|------------------------------|

| | | |
|-----------------|-----------|--|
| Command History | Release | Modification |
| | 12.0(26)S | This command was introduced. |
| | 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

| | |
|------------------|---|
| Usage Guidelines | When Protocol Independent Multicast (PIM) sends multiple joins and prunes simultaneously, it aggregates them into a single packet. The show ipv6 pim join-prune statistic command displays the average number of joins and prunes that were aggregated into a single packet over the last 1000 PIM join-prune packets, over the last 10,000 PIM join-prune packets, and over the last 50,000 PIM join-prune packets. |
|------------------|---|

| | |
|----------|---|
| Examples | The following example provides the join/prune aggregation on Ethernet interface 0/0/0: Router# show ipv6 pim join-prun statistic Ethernet0/0/0 PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets Interface Transmitted Received Ethernet0/0/0 0 / 0 / 0 1 / 0 / 0 |
|----------|---|

show ipv6 pim neighbor

To display the Protocol Independent Multicast (PIM) neighbors discovered by the Cisco IOS software, use the **show ipv6 pim neighbor** command in privileged EXEC mode.

show ipv6 pim neighbor [**detail**] [*interface-type interface-number* | **count**]

| Syntax Description | detail | (Optional) Shows the additional addresses of the neighbors learned, if any, through the routable address hello option. |
|--------------------|--|--|
| | <i>interface-type</i> <i>interface-number</i> | (Optional) Interface type and number. |
| | count | (Optional) Displays neighbor counts on each interface. |

| Command Modes | Privileged EXEC |
|---------------|-----------------|
|---------------|-----------------|

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

| Usage Guidelines | The show ipv6 pim neighbor command displays which routers on the LAN are configured for PIM. |
|------------------|---|
|------------------|---|

Examples The following is sample output from the **show ipv6 pim neighbor** command using the **detail** keyword to identify the additional addresses of the neighbors learned through the routable address hello option:

```
Router# show ipv6 pim neighbor detail
```

```
Neighbor Address(es)      Interface      Uptime      Expires DR pri Bidir
FE80::A8BB:CCFF:FE00:401  Ethernet0/0   01:34:16   00:01:16  1      B
60::1:1:3
FE80::A8BB:CCFF:FE00:501  Ethernet0/0   01:34:15   00:01:18  1      B
60::1:1:4
```

Table 97 describes the significant fields shown in the display.

Table 97 *show ipv6 pim neighbor Field Descriptions*

| Field | Description |
|------------------|---|
| Neighbor Address | IPv6 address of the PIM neighbor. |
| Interface | Interface type and number on which the neighbor is reachable. |
| Uptime | How long (in hours, minutes, and seconds) the entry has been in the PIM neighbor table. |

Table 97 *show ipv6 pim neighbor Field Descriptions (continued)*

| Field | Description |
|---------|--|
| Expires | How long (in hours, minutes, and seconds) until the entry will be removed from the IPv6 multicast routing table. |
| DR | Indicates that this neighbor is a designated router on the LAN. |
| Pri | DR priority used by this neighbor. |
| Bidir | The neighbor is capable of PIM in bidirectional mode. |

Related Commands

| Command | Description |
|--------------------------------|---|
| show ipv6 pim interface | Displays information about interfaces configured for PIM. |

show ipv6 pim range-list

To display information about IPv6 multicast range lists, use the **show ipv6 pim range-list** command in privileged EXEC mode.

show ipv6 pim range-list [**config**] [*rp-address* | *rp-name*]

| | | |
|---------------------------|------------------------------------|---|
| Syntax Description | config | (Optional) The client. Displays the range lists configured on the router. |
| | <i>rp-address</i> <i>rp-name</i> | (Optional) The address of a Protocol Independent Multicast (PIM) rendezvous point (RP). |

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

| | |
|-------------------------|--|
| Usage Guidelines | The show ipv6 pim range-list command displays IPv6 multicast range lists on a per-client and per-mode basis. A client is the entity from which the specified range list was learned. The clients can be config, and the modes can be Source Specific Multicast (SSM) or sparse mode (SM). |
|-------------------------|--|

| | |
|-----------------|--|
| Examples | The following is sample output from the show ipv6 pim range-list command: |
|-----------------|--|

```
Router# show ipv6 pim range-list

config SSM Exp:never Learnt from :::
FF33::/32 Up:00:26:33
FF34::/32 Up:00:26:33
FF35::/32 Up:00:26:33
FF36::/32 Up:00:26:33
FF37::/32 Up:00:26:33
FF38::/32 Up:00:26:33
FF39::/32 Up:00:26:33
FF3A::/32 Up:00:26:33
FF3B::/32 Up:00:26:33
FF3C::/32 Up:00:26:33
FF3D::/32 Up:00:26:33
FF3E::/32 Up:00:26:33
FF3F::/32 Up:00:26:33
config SM RP:40::1:1:1 Exp:never Learnt from :::
FF13::/64 Up:00:03:50
config SM RP:40::1:1:3 Exp:never Learnt from :::
FF09::/64 Up:00:03:50
```

Table 98 describes the significant fields shown in the display.

Table 98 *show ipv6 pim range-list Field Descriptions*

| Field | Description |
|-----------|-----------------------|
| config | Config is the client. |
| SSM | Protocol being used. |
| FF33::/32 | Group range. |
| Up: | Uptime. |

show ipv6 pim topology

To display Protocol Independent Multicast (PIM) topology table information for a specific group or all groups, use the **show ipv6 pim topology** command in privileged EXEC mode.

show ipv6 pim topology [**link-local** | **route-count** | *group-name* | *group-address*] [*source-address* | *source-name*]

| | | |
|---------------------------|--|---|
| Syntax Description | link-local | (Optional) Displays the link-local groups. |
| | route-count | (optional) Number of routes in PIM topology table. |
| | <i>group-name</i> <i>group-address</i> | (Optional) IPv6 address or name of the multicast group. |
| | <i>source address</i> <i>source-name</i> | (Optional) IPv6 address or name of the source. |

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.3(2)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | The link-local keyword was added. |
| | 12.3(4)T | This command was updated in Cisco IOS Release 12.3(4)T. |

Usage Guidelines

This command shows the PIM topology table for a given group—(*, G), (S, G) and (S, G) RPT— as internally stored in a PIM topology table. The PIM topology table may have various entries for a given group, each with its own interface list. The resulting forwarding state is maintained in the MRIB table, which shows which interface the data packet should be accepted on and which interfaces the data packet should be forwarded to for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

The **route-count** keyword shows the count of all entries, including link-local entries.

PIM communicates the contents of these entries through the Multicast Routing Information Base (MRIB), which is an intermediary for communication between multicast routing protocols (such as PIM), local membership protocols (such as Multicast Listener Discovery [MLD]), and the multicast forwarding engine of the system.

For example, an interface is added to (*,G) entry in PIM topology table upon receipt of an MLD report or PIM (*,G) join message. Similarly, an interface is added to (S,G) entry upon receipt of MLD INCLUDE report for S and G or PIM (S,G) join message. Then PIM installs an (S,G) entry in MRIB with immediate olist (from (S,G)) and inherited olist (from (*,G)). Therefore, the proper forwarding state for a given entry (S,G) can be seen only in the MRIB or the MFIB, not in the PIM topology table.

Examples

The following is sample output from the **show ipv6 pim topology** command:

Router# **show ipv6 pim topology**

```
IP PIM Multicast Topology Table
Entry state: (*S,G) [RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
             RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
             RR - Register Received, SR - Sending Registers, E - MSDP External,
             DCC - Don't Check Connected
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
                II - Internal Interest, ID - Internal Dissinterest,
                LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,FF05::1)
SM UP:02:26:56 JP:Join(now) Flags:LH
RP:40::1:1:2
RPF:Ethernet1/1,FE81::1
   Ethernet0/1           02:26:56   fwd LI LH

(50::1:1:200,FF05::1)
SM UP:00:00:07 JP:Null(never) Flags:
RPF:Ethernet1/1,FE80::30:1:4
   Ethernet1/1           00:00:07   off LI
```

Table 99 describes the significant fields shown in the display.

Table 99 *show ipv6 pim topology Field Descriptions*

| Field | Description |
|------------------|---|
| Entry flags: KAT | The keepalive timer (KAT) associated with a source is used to keep track of two intervals while the source is alive. When a source first becomes active, the first-hop router sets the keepalive timer to 3 minutes and 30 seconds, during which time it does not probe to see if the source is alive. Once this timer expires, the router enters the probe interval and resets the timer to 65 seconds during which time the router “assumes” the source is alive and starts probing to determine if it actually is. If the router determines that the source is alive, the router exits the probe interval and resets the keepalive timer to 3 minutes and 30 seconds. If the source is not alive, the entry is deleted at the end of the probe interval. |
| AA, PA | The assume alive (AA) and probe alive (PA) flags are set when the router is in the probe interval for a particular source. |
| RR | The register received (RR) flag is set on the (S, G) entries on the RP as long as the RP receives registers from the source DR, which keeps the source state alive on the RP. |
| SR | The sending registers (SR) flag is set on the (S, G) entries on the DR as long as it sends registers to the RP. |

Related Commands

| Command | Description |
|------------------------------|---|
| show ipv6 mrib client | Displays information about the clients of the MRIB. |
| show ipv6 mrib route | Displays the MRIB route information. |

show ipv6 pim traffic

To display the Protocol Independent Multicast (PIM) traffic counters, use the **show ipv6 pim traffic** command in user EXEC or privileged EXEC mode.

show ipv6 pim traffic

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|--|
| | 12.0(26)S | This command was introduced. |
| | 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines Use the **show ipv6 pim traffic** command to check if the expected number of PIM protocol messages have been received and sent.

Examples The following example shows the number of PIM protocol messages received and sent.

```
Router# show ipv6 pim traffic

PIM Traffic Counters
Elapsed time since counters cleared:00:05:29

Valid PIM Packets      Received      Sent
Hello                  22            22
Join-Prune              0             0
Register                0             0
Register Stop           0             0
Assert                  0             0
Bidir DF Election       0             0

Errors:
Malformed Packets                0
Bad Checksums                     0
Send Errors                       0
Packet Sent on Loopback Errors    0
Packets Received on PIM-disabled Interface 0
Packets Received with Unknown PIM Version 0
```

Table 100 describes the significant fields shown in the display.

Table 100 *show ipv6 pim traffic Field Descriptions*

| Field | Description |
|-------------------------------------|---|
| Elapsed time since counters cleared | Indicates the amount of time (in hours, minutes, and seconds) since the counters cleared. |
| Valid PIM Packets | Number of valid PIM packets received and sent. |
| Hello | Number of valid hello messages received and sent. |
| Join-Prune | Number of join and prune announcements received and sent. |
| Register | Number of PIM register messages received and sent. |
| Register Stop | Number of PIM register stop messages received and sent. |
| Assert | Number of asserts received and sent. |

show ipv6 pim tunnel

To display information about the Protocol Independent Multicast (PIM) register encapsulation and de-encapsulation tunnels on an interface, use the **show ipv6 pim tunnel** command in privileged EXEC mode.

show ipv6 pim tunnel [*interface-type interface-number*]

Syntax Description

interface-type (Optional) Tunnel interface type and number.
interface-number

Command Modes

Privileged EXEC

Command History

| Release | Modification |
|-----------|---|
| 12.3(2)T | This command was introduced. |
| 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines

If you use the **show ipv6 pim tunnel** command without the optional *interface* keyword, information about the PIM register encapsulation and de-encapsulation tunnel interfaces is displayed.

The PIM encapsulation tunnel is the register tunnel. An encapsulation tunnel is created for every known rendezvous point (RP) on each router. The PIM decapsulation tunnel is the register decapsulation tunnel. A decapsulation tunnel is created on the RP for the address that is configured to be the RP address.

Examples

The following is sample output from the **show ipv6 pim tunnel** command on the RP:

```
Router# show ipv6 pim tunnel

Tunnel0*
  Type   :PIM Encap
  RP     :100::1
  Source:100::1
Tunnel0*
  Type   :PIM Decap
  RP     :100::1
  Source: -
```

The following is sample output from the **show ipv6 pim tunnel** command on a non-RP:

```
Router# show ipv6 pim tunnel

Tunnel0*
  Type   :PIM Encap
  RP     :100::1
  Source:2001::1:1:1
```

Table 101 describes the significant fields shown in the display.

Table 101 *show ipv6 pim tunnel Field Descriptions*

| Field | Description |
|----------|---|
| Tunnel0* | Name of the tunnel. |
| Type | Type of tunnel. Can be PIM encapsulation or PIM de-encapsulation. |
| source | Source address of the router that is sending encapsulating registers to the RP. |

show ipv6 prefix-list

To display information about an IPv6 prefix list or IPv6 prefix list entries, use the **show ipv6 prefix-list** command in user EXEC or privileged EXEC mode.

show ipv6 prefix-list [**detail** | **summary**] [*list-name*]

show ipv6 prefix-list *list-name* *ipv6-prefix/prefix-length* [**longer** | **first-match**]

show ipv6 prefix-list *list-name* **seq** *seq-num*

| Syntax Description | | |
|--------------------|--------------------------------|---|
| | detail summary | (Optional) Displays detailed or summarized information about all IPv6 prefix lists. |
| | <i>list-name</i> | (Optional) The name of a specific IPv6 prefix list. |
| | <i>ipv6-prefix</i> | (Optional) All prefix list entries for the specified IPv6 network. 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> | (Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |
| | longer | (Optional) Displays all entries of an IPv6 prefix list that are more specific than the given <i>ipv6-prefix/prefix-length</i> values. |
| | first-match | (Optional) Displays the entry of an IPv6 prefix list that matches the given <i>ipv6-prefix/prefix-length</i> values. |
| | seq <i>seq-num</i> | (Optional) The sequence number of the IPv6 prefix list entry. |

Defaults Displays information about all IPv6 prefix lists.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines The **show ipv6 prefix-list** command provides output similar to the **show ip prefix-list** command, except that it is IPv6-specific.

Examples

The following example shows the output of the **show ipv6 prefix-list** command with the **detail** keyword:

```
Router# show ipv6 prefix-list detail

Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
  count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
  seq 5 permit 2002::/16 (hit count: 313, refcount: 1)
ipv6 prefix-list aggregate:
  count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
  seq 5 deny 3FFE:C00::/24 ge 25 (hit count: 568, refcount: 1)
  seq 10 permit ::/0 le 48 (hit count: 31310, refcount: 1)
ipv6 prefix-list bgp-in:
  count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
  seq 5 deny 5F00::/8 le 128 (hit count: 0, refcount: 1)
  seq 10 deny ::/0 (hit count: 0, refcount: 1)
  seq 15 deny ::/1 (hit count: 0, refcount: 1)
  seq 20 deny ::/2 (hit count: 0, refcount: 1)
  seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
  seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)
```

Table 102 describes the significant fields shown in the display.

Table 102 show ipv6 prefix-list Field Descriptions

| Field | Description |
|---|---|
| Prefix list with the latest deletion/insertion: | Prefix list that was last modified. |
| count | Number of entries in the list. |
| range entries | Number of entries with matching range. |
| sequences | Sequence number for the prefix entry. |
| refcount | Number of objects currently using this prefix list. |
| seq | Entry number in the list. |
| permit, deny | Granting status. |
| hit count | Number of matches for the prefix entry. |

The following example shows the output of the **show ipv6 prefix-list** command with the **summary** keyword.

```
Router# show ipv6 prefix-list summary

Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
  count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
ipv6 prefix-list aggregate:
  count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
ipv6 prefix-list bgp-in:
  count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
```

Related Commands

| Command | Description |
|-------------------------------|--|
| clear ipv6 prefix-list | Resets the hit count of the prefix list entries. |
| distribute-list in | Filters networks received in updates. |

| | |
|-------------------------------------|--|
| distribute-list out | Suppresses networks from being advertised in updates. |
| ipv6 prefix-list | Creates an entry in an IPv6 prefix list. |
| ipv6 prefix-list description | Adds a text description of an IPv6 prefix list. |
| match ipv6 address | Distributes IPv6 routes that have a prefix permitted by a prefix list. |
| neighbor prefix-list | Distributes BGP neighbor information as specified in a prefix list. |
| remark (prefix-list) | Adds a comment for an entry in a prefix list. |

show ipv6 protocols

To display the parameters and current state of the active IPv6 routing protocol processes, use the **show ipv6 protocols** command in EXEC mode.

show ipv6 protocols [summary]

| | |
|---------------------------|---|
| Syntax Description | summary (Optional) Displays the configured routing protocol process names. |
|---------------------------|---|

| | |
|----------------------|------|
| Command Modes | EXEC |
|----------------------|------|

| Command History | Release | Modification |
|------------------------|------------|--|
| | 12.2(8)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

| | |
|-------------------------|--|
| Usage Guidelines | The information displayed by the show ipv6 protocols command is useful in debugging routing operations. |
|-------------------------|--|

| | |
|-----------------|--|
| Examples | The following is sample output from the show ipv6 protocols command, showing Intermediate System-to-Intermediate System (IS-IS) routing protocol information: |
|-----------------|--|

```
Router# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"
  Interfaces:
    Ethernet0/0/3
    Ethernet0/0/1
    Serial1/0/1
    Loopback1 (Passive)
    Loopback2 (Passive)
    Loopback3 (Passive)
    Loopback4 (Passive)
    Loopback5 (Passive)
  Redistribution:
    Redistributing protocol static at level 1
  Inter-area redistribution
    Redistributing L1 into L2 using prefix-list word
  Address Summarization:
    L2: 33::/16 advertised with metric 0
    L2: 44::/16 advertised with metric 20
    L2: 66::/16 advertised with metric 10
    L2: 77::/16 advertised with metric 10
```

Table 103 describes the significant fields shown in the display.

Table 103 *show ipv6 protocols Field Descriptions for IS-IS Processes*

| Field | Description |
|---------------------------|---|
| IPv6 Routing Protocol is | Specifies the IPv6 routing protocol used. |
| Interfaces | Specifies the interfaces on which the IPv6 IS-IS protocol is configured. |
| Redistribution | Lists the protocol that is being redistributed. |
| Inter-area redistribution | Lists the IS-IS levels that are being redistributed into other levels. |
| using prefix-list | Names the prefix list used in the interarea redistribution. |
| Address Summarization | Lists all the summary prefixes. If the summary prefix is being advertised then “advertised with metric <i>x</i> ” will be displayed after the prefix. |

The following is sample output from the **show ipv6 protocols** command, showing Border Gateway Protocol (BGP) routing protocol information for autonomous system 30:

```
Router# show ipv6 protocols
```

```
IPv6 Routing Protocol is "bgp 30"
IGP synchronization is disabled
Redistribution:
  Redistributing protocol connected
Neighbor(s):
  Address                FiltIn FiltOut Weight RoutemapIn RoutemapOut
  2002:3000::36C         5       7    200
  5000::1                rmap-in  rmap-out
  7000::36C              rmap-in  rmap-out
```

Table 104 describes the significant fields shown in the display.

Table 104 *show ipv6 protocols Field Descriptions for BGP Process*

| Field | Description |
|--------------------------|---|
| IPv6 Routing Protocol is | Specifies the IPv6 routing protocol used. |
| Redistribution | Lists the protocol that is being redistributed. |
| Address | Neighbor IPv6 address. |
| FiltIn | AS-path filter list applied to input. |
| FiltOut | AS-path filter list applied to output. |
| Weight | Neighbor weight value used in BGP bestpath selection. |
| RoutemapIn | Neighbor route map applied to input. |
| RoutemapOut | Neighbor route map applied to output. |

The following is sample output from the **show ipv6 protocols** command with the **summary** keyword:

```
Router# show ipv6 protocols summary
```

```
Index Process Name
0      connected
1      static
```

```
2    rip myrip
3    bgp 30
```

show ipv6 rip

To display information about current IPv6 Routing Information Protocol (RIP) processes, use the **show ipv6 rip** command in user EXEC or privileged EXEC mode.

show ipv6 rip [*name*] [**database** | **next-hops**]

| | | |
|---------------------------|------------------|--|
| Syntax Description | <i>name</i> | (Optional) Name of the RIP process. If the name is not entered, details of all configured RIP processes will be displayed. |
| | database | (Optional) Details of the entries in the specified RIP IPv6 routing table are displayed. |
| | next-hops | (Optional) Details of the specified RIP IPv6 processes next hop addresses are displayed. If no RIP process name is specified, the next hop addresses for all RIP IPv6 processes will be displayed. |

Defaults Information about all current IPv6 RIP processes is displayed.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|------------------------|----------------|---|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.2(22)S and the <i>name</i> argument and the database and next-hops keywords were added. |
| | 12.2(13)T | The modifications to add the <i>name</i> argument and the database and next-hops keywords were integrated into this release. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Examples The following is sample output from the **show ipv6 rip** command:

```
Router# show ipv6 rip

RIP process "one", port 521, multicast-group FF02::9, pid 55
  Administrative distance is 25. Maximum paths is 4
  Updates every 30 seconds, expire after 180
  Holddown lasts 0 seconds, garbage collect after 120
  Split horizon is on; poison reverse is off
  Default routes are not generated
  Periodic updates 8883, trigger updates 2
  Interfaces:
    Ethernet2
  Redistribution:
RIP process "two", port 521, multicast-group FF02::9, pid 61
  Administrative distance is 120. Maximum paths is 4
  Updates every 30 seconds, expire after 180
```

```

Holddown lasts 0 seconds, garbage collect after 120
Split horizon is on; poison reverse is off
Default routes are not generated
Periodic updates 8883, trigger updates 0
Interfaces:
  None
Redistribution:

```

Table 105 describes the significant fields shown in the display.

Table 105 *show ipv6 rip Field Descriptions*

| Field | Description |
|-------------------------|---|
| RIP process | The name of the RIP process. |
| port | The port that the RIP process is using. |
| multicast-group | The IPv6 multicast group of which the RIP process is a member. |
| pid | The process identification number (pid) assigned to the RIP process. |
| Administrative distance | Used to rank the preference of sources of routing information. Connected routes have an administrative distance of 1 and are preferred over the same route learned by a protocol with a larger administrative distance value. |
| Updates | The value (in seconds) of the update timer. |
| expire | The interval (in seconds) in which updates expire. |
| Holddown | The value (in seconds) of the hold-down timer. |
| garbage collect | The value (in seconds) of the garbage-collect timer. |
| Split horizon | The split horizon state is either on or off. |
| poison reverse | The poison reverse state is either on or off. |
| Default routes | The origination of a default route into RIP. Default routes are either generated or not generated. |
| Periodic updates | The number of RIP update packets sent on an update timer. |
| trigger updates | The number of RIP update packets sent as triggered updates. |

To display information about a specified IPv6 RIP process database, enter the **show ipv6 rip EXEC** command with the *name* argument and the **database** keyword. In the following output for the IPv6 RIP process named one, timer information is displayed, and route 3004::/64 has a route tag set:

```
Router# show ipv6 rip one database
```

```

RIP process "one", local RIB
2001:72D:1000::/64, metric 2
  Ethernet2/FE80::202:7DFF:FE1A:9472, expires in 168 secs
2001:72D:2000::/64, metric 2, installed
  Ethernet2/FE80::202:7DFF:FE1A:9472, expires in 168 secs
2001:72D:3000::/64, metric 2, installed
  Ethernet2/FE80::202:7DFF:FE1A:9472, expires in 168 secs
  Ethernet1/FE80::203:7EBC:FE23:1000, expires in 120 secs
2001:72D:4000::/64, metric 16, expired, [advertise 119/hold 0]
  Ethernet2/FE80::202:7DFF:FE1A:9472
3004::/64, metric 2 tag 2A, installed
  Ethernet2/FE80::202:7DFF:FE1A:9472, expires in 168 secs

```

Table 106 describes the significant fields shown in the display.

Table 106 show ipv6 rip database Field Descriptions

| Field | Description |
|------------------------------------|--|
| RIP process | The name of the RIP process. |
| 2001:72D:1000::/64 | The IPv6 route prefix. |
| metric | Metric for the route. |
| installed | Route is installed in the IPv6 routing table. |
| Ethernet2/FE80::202:7DFF:FE1A:9472 | Interface and LL next hop through which the IPv6 route was learned. |
| expires in | The interval (in seconds) before the route expires. |
| advertise | For an expired route, the value (in seconds) during which the route will be advertised as expired. |
| hold | The value (in seconds) of the hold-down timer. |
| tag | Route tag. |

To display information about the next-hops for a specified IPv6 RIP process, enter the **show ipv6 rip EXEC** command with the *name* argument and the **next-hops** keyword:

```
Router# show ipv6 rip one next-hops
```

```
RIP process "one", Next Hops
  FE80::210:7BFF:FEC2:ACCF/Ethernet4/2 [1 routes]
  FE80::210:7BFF:FEC2:B286/Ethernet4/2 [2 routes]
```

Table 107 describes the significant fields shown in the display.

Table 107 show ipv6 rip next-hops Field Descriptions

| Field | Description |
|--------------------------------------|--|
| RIP process | The name of the RIP process. |
| FE80::210:7BFF:FEC2:ACCF/Ethernet4/2 | The next hop address and interface through which it was learned. Next hops are either the addresses of IPv6 RIP neighbors from which we have learned routes, or explicit next hops received in IPv6 RIP advertisements. Note An IPv6 RIP neighbor may choose to advertise all its routes with an explicit next hop. In this case the address of the neighbor would not appear in the next hop display. |
| [1 routes] | The number of routes in the IPv6 RIP routing table using the specified next hop. |

show ipv6 route

To display the current contents of the IPv6 routing table, use the **show ipv6 route** command in user EXEC or privileged EXEC mode.

```
show ipv6 route [ipv6-address | ipv6-prefix/prefix-length | protocol | interface-type
                 interface-number]
```

| | | |
|--------------------|------------------|--|
| Syntax Description | ipv6-address | (Optional) Displays routing information for a specific IPv6 address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| | ipv6-prefix | (Optional) Displays routing information for a specific IPv6 network. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| | lprefix-length | (Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |
| | protocol | (Optional) Displays routes for the specified routing protocol using any of these keywords: bgp, isis, ospf, or rip; or displays routes for the specified type of route using any of these keywords: connected, local, static, or the interface keyword for a specific interface. |
| | interface-type | (Optional) Interface type. For more information about supported interface types, use the question mark (?) online help function. |
| | interface-number | (Optional) Interface number. For more information about the numbering syntax for supported interface types, use the question mark (?) online help function. |

Defaults All IPv6 routing information for all active routing tables is displayed.

Command Modes User EXEC
Privileged EXEC

| | | |
|-----------------|------------|--|
| Command History | Release | Modification |
| | 12.2(2)T | This command was introduced. |
| | 12.2(8)T | The isis protocol keyword was added to the command syntax, and the I1 - ISIS L1, I2 - ISIS L2, and IA - ISIS interarea fields were added to the command output. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |

| Release | Modification |
|-----------|--|
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S, the timer information was removed, and an indicator was added to display IPv6 MPLS virtual interfaces. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T, the timer information was removed, and an indicator was added to display IPv6 MPLS virtual interfaces. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S and support for longer prefixes was added. |

Usage Guidelines

The **show ipv6 route** command provides output similar to the **show ip route** command, except that the information is IPv6-specific.

When the *ipv6-address* or *ipv6-prefix/prefix-length* argument is specified, a longest match lookup is performed from the routing table and only route information for that address or network is displayed. When a routing protocol is specified, only routes for that protocol are displayed. When the **connected**, **local**, or **static** keyword is specified, only that type of route is displayed. When the *interface-type* *interface-number* arguments are specified, only the specified interface-specific routes are displayed.

Examples

show ipv6 route Command with No Keyword Specified Example

The following is sample output from the **show ipv6 route** command when entered without an IPv6 address or prefix specified:

```
Router# show ipv6 route

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - IIS interarea
B   3000::/64 [20/0]
    via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
L   4000::2/128 [0/0]
    via ::, Ethernet1/0
C   4000::/64 [0/0]
    via ::, Ethernet1/0
LC  4001::1/128 [0/0]
    via ::, Loopback0
L   5000::2/128 [0/0]
    via ::, Serial6/0
C   5000::/64 [0/0]
    via ::, Serial6/0
S   5432::/48 [1/0]
    via 4000::1, Null
L   FE80::/10 [0/0]
    via ::, Null0
L   FF00::/8 [0/0]
    via ::, Null0
```

Table 108 describes the significant fields shown in the display.

Table 108 show ipv6 route Field Descriptions

| Field | Description |
|--------------------------|---|
| Codes: | Indicates the protocol that derived the route. Values are as follows: C—Connected L—Local S—Static R—RIP derived B—BGP derived I1—ISIS L1—Integrated IS-IS Level 1 derived I2—ISIS L2—Integrated IS-IS Level 2 derived IA—ISIS interarea—Integrated IS-IS interarea derived |
| 2001:0DB8:DDDD::/32 | Indicates the IPv6 prefix of the remote network. |
| [200/0] | The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route. |
| via ::FFFF:192.168.99.70 | Specifies the address of the next router to the remote network. |
| IPv6-mpls | Specifies the interface through which the next router to the specified network can be reached. Note In this example output, the interface is the IPv6 Multiprotocol Label Switching (MPLS) virtual interface used in the 6PE feature where IPv6 traffic is sent across an IPv4 MPLS backbone from one IPv6 provider edge router to another. |

show ipv6 route Command with Address or Prefix Specified Example

When the *ipv6-address* or *ipv6-prefix/prefix-length* argument is specified, only route information for that address or network is displayed. The following is sample output from the **show ipv6 route** command when entered with the IPv6 prefix 2001:200::/35:

```
Router# show ipv6 route 2001:200::/35

IPv6 Routing Table - 261 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

B 2001:200::/35 [20/3]
  via FE80::60:5C59:9E00:16, Tunnel1
```

show ipv6 route Command with Protocol Specified Example

When you specify a protocol, only routes for that particular routing protocol are shown. The following is sample output from the **show ipv6 route** command when entered with the **bgp** keyword:

```
Router# show ipv6 route bgp

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B 3000::/64 [20/0]
  via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
```

show ipv6 route Command for Local Routes Example

```
Router# show ipv6 route local
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
L   4000::2/128 [0/0]
    via ::, Ethernet1/0
LC  4001::1/128 [0/0]
    via ::, Loopback0
L   5000::2/128 [0/0]
    via ::, Serial6/0
L   FE80::/10 [0/0]
    via ::, Null0
L   FF00::/8 [0/0]
    via ::, Null0
```

Related Commands

| Command | Description |
|--------------------------------|--|
| ipv6 route | Establishes a static IPv6 route. |
| show ipv6 interface | Displays IPv6 interface information. |
| show ipv6 route summary | Displays the current contents of the IPv6 routing table in summary format. |
| show ipv6 tunnel | Displays IPv6 tunnel information. |

show ipv6 route summary

To display the current contents of the IPv6 routing table in summary format, use the **show ipv6 route summary** command in user EXEC or privileged EXEC mode.

show ipv6 route summary

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Examples The following is sample output from the **show ipv6 route summary** command:

```
Router# show ipv6 route summary
```

```
IPv6 Routing Table Summary - 257 entries
 37 local, 35 connected, 25 static, 0 RIP, 160 BGP
Number of prefixes:
  /16: 1, /24: 46, /28: 10, /32: 5, /35: 25, /40: 1, /48: 63, /64: 19
  /96: 15, /112: 1, /126: 31, /127: 4, /128: 36
```

Table 109 describes the significant fields shown in the display.

Table 109 show ipv6 route summary Field Descriptions

| Field | Description |
|---------------------|---|
| entries | Number of entries in the IPv6 routing table. |
| Route source | Number of routes that are present in the routing table for each route source, which can be local routes, connected routes, static routes, a routing protocol, prefix and address or name, and longer prefixes and address or name. Routing protocols can include RIP, IS-IS, OSPF, and BGP. Other route sources can be connected, local, static, or a specific interface. |
| Number of prefixes: | Number of routing table entries for given prefix length. |

| Related Commands | Command | Description |
|------------------|-----------------|--|
| | show ipv6 route | Displays the current contents of the IPv6 routing table. |

show ipv6 routers

To display IPv6 router advertisement information received from onlink routers, use the **show ipv6 routers** command in user EXEC or privileged EXEC mode.

show ipv6 routers [*interface-type interface-number*] [**conflicts**]

| | | |
|---------------------------|-------------------------|---|
| Syntax Description | <i>interface-type</i> | (Optional) Specifies the interface type. |
| | <i>interface-number</i> | (Optional) Specifies the interface number. |
| | conflicts | (Optional) Displays router advertisements that differ from the advertisements configured for a specified interface. |

Defaults When an interface is not specified, onlink router advertisement information is displayed for all interface types. (The term *onlink* refers to a locally reachable address on the link.)

Command Modes User EXEC
Privileged EXEC

| | | |
|------------------------|----------------|--|
| Command History | Release | Modification |
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines Routers advertising parameters that differ from the advertisement parameters configured for the interface on which the advertisements are received are marked as conflicting.

Examples The following is sample output from the **show ipv6 routers** command when entered without an IPv6 interface type and number:

```
Router# show ipv6 routers

Router FE80::83B3:60A4 on Tunnel5, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
  Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on Tunnel57, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

Table 110 describes the significant fields shown in the display.

Table 110 show ipv6 routers Field Descriptions

| Field | Description |
|--------------------|---|
| Hops | The configured hop limit value for the router advertisement. |
| Lifetime | The configured Router Lifetime value for the router advertisement. A value of 0 indicates that the router is not a default router. A value other than 0 indicates that the router is a default router. |
| AddrFlag | If the value is 0, the router advertisement received from the router indicates that addresses are not configured using the stateful autoconfiguration mechanism. If the value is 1, the addresses are configured using this mechanism. |
| OtherFlag | If the value is 0, the router advertisement received from the router indicates that information other than addresses is not obtained using the stateful autoconfiguration mechanism. If the value is 1, other information is obtained using this mechanism. (The value of OtherFlag can be 1 only if the value of AddrFlag is 1.) |
| Reachable time | The configured ReachableTimer value for the router advertisement. The time value to be used on this link for neighbor unreachability detection. A value of 0 indicates that it is not specified by the advertising router. |
| Retransmit time | The configured RetransTimer value. The time value to be used on this link for neighbor solicitation transmissions, which are used in address resolution and neighbor unreachability detection. A value of 0 means the time value is not specified by the advertising router. |
| Prefix | A prefix advertised by the router. Also indicates if onlink or autoconfig bits were set in the router advertisement message. |
| Valid lifetime | The length of time (in seconds) relative to the time the advertisement is sent that the prefix is valid for the purpose of onlink determination. A value of -1 (all ones, 0xffffffff) represents infinity. |
| preferred lifetime | The length of time (in seconds) relative to the time the advertisements is sent that addresses generated from the prefix via address autoconfiguration remain valid. A value of -1 (all ones, 0xffffffff) represents infinity. |

When the *interface-type* and *interface-number* arguments are specified, router advertisement details about that specific interface are displayed. The following is sample output from the **show ipv6 routers** command when entered with an interface type and number:

```
Router# show ipv6 routers tunnel 5

Router FE80::83B3:60A4 on Tunnel5, last update 5 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
  Valid lifetime -1, preferred lifetime -1
```

Entering the **conflicts** keyword with the **show ipv6 routers** command displays information for routers that are advertising parameters different from the parameters configured for the interface on which the advertisements are being received, as the following sample output shows:

```
Router# show ipv6 routers conflicts

Router FE80::203:FDFE:FE34:7039 on Ethernet1, last update 1 min, CONFLICT
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

```
Prefix 2003::/64 onlink autoconfig
  Valid lifetime -1, preferred lifetime -1
Router FE80::201:42FF:FECA:A5C on Ethernet1, last update 0 min, CONFLICT
Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
Reachable time 0 msec, Retransmit time 0 msec
Prefix 2001::/64 onlink autoconfig
  Valid lifetime -1, preferred lifetime -1
```

show ipv6 rpf

To check Reverse Path Forwarding (RPF) information for a given unicast host address and prefix, use the **show ipv6 rpf** command in user EXEC and privileged EXEC mode.

```
show ipv6 rpf ipv6-prefix
```

| | |
|--------------------|---|
| Syntax | Description |
| <i>ipv6-prefix</i> | Summary prefix designated for a range of IPv6 prefixes. The <i>ipv6-prefix</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |

| | |
|---------------|------------------------------|
| Command Modes | User EXEC Privileged EXEC |
|---------------|------------------------------|

| | | |
|-----------------|-----------|--|
| Command History | Release | Modification |
| | 12.0(26)S | This command was introduced. |
| | 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

Usage Guidelines

The **show ipv6 rpf** command displays how IPv6 multicast routing performs RPF. Because the router can find RPF information from multiple routing tables (for example, unicast routing information base [RIB], multiprotocol Border Gateway Protocol [MBGP] routing table, or static mroutes), the **show ipv6 rpf** command displays from where the information is retrieved.

Examples

The following example displays RPF information for the unicast host with the IPv6 address of 2001::1:1:2:

```
Router# show ipv6 rpf 2001::1:1:2

RPF information for 2001::1:1:2
RPF interface:Ethernet3/2
RPF neighbor:FE80::40:1:3
RPF route/mask:20::/64
RPF type:Unicast
RPF recursion count:0
Metric preference:110
Metric:30
```


show ipv6 static

To display the current contents of the IPv6 routing table, use the **show ipv6 static** command in user EXEC or privileged EXEC mode.

```
show ipv6 static [ipv6-address | ipv6-prefix/prefix-length][interface interface-type
interface-number] [recursive] [detail]
```

| Syntax Description | | |
|-------------------------|---|--|
| <i>ipv6-address</i> | (Optional) Displays routing information for a specific IPv6 address. | 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>ipv6-prefix</i> | (Optional) Displays routing information for a specific IPv6 network. | 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> | (Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. | |
| interface | (Optional) Name of a routing protocol, or the connected , local , or static keyword. If you specify a routing protocol, use the bgp , isis , or rip keyword. | |
| <i>interface-type</i> | (Optional, but required if interface keyword is used) Interface type. For a list of supported interface types, use the question mark (?) online help function. | |
| <i>interface-number</i> | (Optional, but required if interface keyword is used) Interface number. For specific numbering syntax for supported interface types, use the question mark (?) online help function. | |

Defaults All IPv6 routing information for all active routing tables is displayed.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|----------|--|
| | 12.3(4)T | This command was introduced through DDTS CSCuk41339. |

Usage Guidelines The **show ipv6 static** command provides output similar to the **show ip route** command, except that it is IPv6-specific.

When the *ipv6-address* or *ipv6-prefix/prefix-length* argument is specified, a longest match lookup is performed from the routing table and only route information for that address or network is displayed. Only the information matching the criteria specified in the command syntax is displayed. For example, when the *interface-type interface-number* arguments are specified, only the specified interface-specific routes are displayed.

Using recursive and interface Keywords

The recursive and interface keywords are mutually exclusive, but they can each be used when the IPv6 prefix is specified in the command statement.

Examples

show ipv6 static with No Options Specified in the Command Syntax Example

When no options specified in the command, those routes installed in the IPv6 routing information base (RIB) are marked with an asterisk, as shown in the following example:

```
Router#sho ipv6 static
IPv6 Static routes
Code: * - installed in RIB
* 3000::/16, interface Ethernet1/0, distance 1
* 4000::/16, via nexthop 2001:1::1, distance 1
  5000::/16, interface Ethernet3/0, distance 1
* 5555::/16, via nexthop 4000::1, distance 1
  5555::/16, via nexthop 9999::1, distance 1
* 5555::/16, interface Ethernet2/0, distance 1
* 6000::/16, via nexthop 2007::1, interface Ethernet1/0, distance 1
```

Table 108 describes the significant fields shown in the display.

Table 111 *show ipv6 static Field Descriptions*

| Field | Description |
|---------------------|---|
| Codes: | Indicates the protocol that derived the route. Values are as follows: C—Connected L—Local S—Static R—RIP derived B—BGP derived I1—ISIS L1—Integrated IS-IS Level 1 derived I2—ISIS L2—Integrated IS-IS Level 2 derived IA—ISIS interarea—Integrated IS-IS interarea derived |
| 2001:0DB8:DDDD::/32 | Indicates the IPv6 prefix of the remote network. |
| via nexthop | Specifies the address of the next router in the path to the remote network. |
| distance <i>n</i> | Indicates the administrative distance to the specified route. |

show ipv6 static With the IPv6 Address and Prefix Example

When the *ipv6-address* or *ipv6-prefix/prefix-length* argument is specified, only information about static routes for that address or network is displayed. The following is sample output from the **show ipv6 route** command when entered with the IPv6 prefix 2001:200::/35:

```
Router# show ipv6 static 2001:200::/35
IPv6 Static routes
Code: * - installed in RIB
* 2001:200::/35, via nexthop 4000::1, distance 1
  2001:200::/35, via nexthop 9999::1, distance 1
* 2001:200::/35, interface Ethernet2/0, distance 1
```

show ipv6 static interface Example

When an interface is supplied, only those static routes with the specified interface as outgoing interface are displayed. The **interface** keyword may be used with or without the IPv6 address and prefix specified in the command statement.

```
Router# show ipv6 static interface e3/0
IPv6 Static routes
Code: * - installed in RIB
  5000::/16, interface Ethernet3/0, distance 1
```

show ipv6 static recursive Example

When the **recursive** keyword is specified, only recursive static routes are displayed. The **recursive** keyword is mutually exclusive with the **interface** keyword, but it may be used *with* or *without* the IPv6 prefix included in the command syntax.

```
Router# show ipv6 static recursive
IPv6 Static routes
Code: * - installed in RIB
* 4000::/16, via nexthop 2001:1::1, distance 1
* 5555::/16, via nexthop 4000::1, distance 1
  5555::/16, via nexthop 9999::1, distance 1
```

show ipv6 static detail Example

When the **detail** keyword is specified, the following additional information is also displayed:

- For *valid* recursive routes, the output path set, and maximum resolution depth
- For *invalid* recursive routes, the reason why the route is not valid.
- For *invalid* direct or fully-specified routes, the reason why the route is not valid.

```
Router# show ipv6 static detail
IPv6 Static routes
Code: * - installed in RIB
* 3000::/16, interface Ethernet1/0, distance 1
* 4000::/16, via nexthop 2001:1::1, distance 1
  Resolves to 1 paths (max depth 1)
  via Ethernet1/0
  5000::/16, interface Ethernet3/0, distance 1
  Interface is down
* 5555::/16, via nexthop 4000::1, distance 1
  Resolves to 1 paths (max depth 2)
  via Ethernet1/0
  5555::/16, via nexthop 9999::1, distance 1
  Route does not fully resolve
* 5555::/16, interface Ethernet2/0, distance 1
* 6000::/16, via nexthop 2007::1, interface Ethernet1/0, distance 1
```

Related Commands

| Command | Description |
|--------------------------------|--|
| ipv6 route | Establishes a static IPv6 route. |
| show ipv6 interface | Displays IPv6 interface information. |
| show ipv6 route summary | Displays the current contents of the IPv6 routing table in summary format. |
| show ipv6 tunnel | Displays IPv6 tunnel information. |

show ipv6 traffic

To display statistics about IPv6 traffic, use the **show ipv6 traffic** command in user EXEC mode.

show ipv6 traffic

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S and output fields were added. |
| | 12.2(13)T | The modification to add output fields was integrated into this release. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines The **show ipv6 traffic** command provides output similar to the **show ip traffic** command, except that it is IPv6-specific.

Examples The following is sample output from the **show ipv6 traffic** command:

```
Router# show ipv6 traffic
```

```
IPv6 statistics:
```

```
  Rcvd:  545 total, 545 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         218 fragments, 109 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  228 generated, 0 forwarded
         1 fragmented into 2 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 168 received, 70 sent
```

```
ICMP statistics:
```

```
  Rcvd: 116 input, 0 checksum errors, 0 too short
         0 unknown info type, 0 unknown error type
  unreachable: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
  parameter: 0 error, 0 header, 0 option
         0 hopcount expired, 0 reassembly timeout, 0 too big
         0 echo request, 0 echo reply
         0 group query, 0 group report, 0 group reduce
         0 router solicit, 60 router advert, 0 redirects
         31 neighbor solicit, 25 neighbor advert
```

```

Sent: 85 output, 0 rate-limited
      unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
      parameter: 0 error, 0 header, 0 option
      0 hopcount expired, 0 reassembly timeout, 0 too big
      0 echo request, 0 echo reply
      0 group query, 0 group report, 0 group reduce
      0 router solicit, 18 router advert, 0 redirects
      33 neighbor solicit, 34 neighbor advert

```

UDP statistics:

```

Rcvd: 109 input, 0 checksum errors, 0 length errors
      0 no port, 0 dropped
Sent: 37 output

```

TCP statistics:

```

Rcvd: 85 input, 0 checksum errors
Sent: 103 output, 0 retransmitted

```

Table 112 describes the significant fields shown in the display.

Table 112 *show ipv6 traffic Field Descriptions*

| Field | Description |
|--|---|
| source-routed | Number of source-routed packets. |
| truncated | Number of truncated packets. |
| format errors | Errors that can result from checks performed on header fields, the version number, and packet length. |
| not a router | Message sent when IPv6 unicast routing is not enabled. |
| bad hop count (not shown in sample output) | Occurs when a packet is discarded because its time-to-live (TTL) field was decremented to zero. |
| failed | Number of failed fragment transmissions. |
| encapsulation failed | Failure that can result from an unresolved address or try-and-queue packet. |
| no route | Counted when the software discards a datagram it did not know how to route. |
| unreach | Unreachable messages received are as follows: <ul style="list-style-type: none"> • routing—Indicates no route to the destination. • admin—Indicates that communication with the destination is administratively prohibited. • neighbor—Indicates that the destination is beyond the scope of the source address. For example, the source may be a local site or the destination may not have a route back to the source. • address—Indicates that the address is unreachable. • port—Indicates that the port is unreachable. |

show ipv6 tunnel

To display IPv6 tunnel information, use the **show ipv6 tunnel** command in user EXEC or privileged EXEC mode.

show ipv6 tunnel

Syntax Description This command has no keywords or arguments

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines For each tunnel running IPv6, use the **show ipv6 tunnel** command to display the tunnel unit number, the name of the dynamic routing protocol used by the tunnel, the time of last input, the number of packets in the last input, and the description string as set by the **description** command.

Examples The following is sample output from the **show ipv6 tunnel** command:

Router# **show ipv6 tunnel**

```
Tun Route  LastInp  Packets
0  RIPng    never      0
1  -        00:00:13  55495
2  -        never     0
3  -        00:00:21  14755
4  -        never     0
5  -        00:00:00  15840
6  -        never     0
7  -        00:00:18  16008
8  -        never     0
9  -        never     0
10 -        never     0
11 -        00:00:03  94801
12 -        1d02h      2
13 -        never     0
14 -        00:00:08  312190
15 -        never     0
16 -        never     0
17 -        never     0
18 -        00:00:05  1034954
19 -        never     0
20 -        00:00:01  1171114
```

```
21      -          never          0
```

Table 113 describes the significant fields shown in the display.

Table 113 *show ipv6 tunnel Field Descriptions*

| Field | Description |
|--|---|
| Tun | Tunnel number. |
| Route | Indicates whether IPv6 RIP is enabled (RIPng) on this tunnel interface or is not enabled (-). |
| Last Inp | Time of last input into the tunnel. |
| Packets | Number of packets in this tunnel. |
| Description (not shown in sample output) | Description of the tunnel as entered in interface configuration mode. |

show isis database

To display the Intermediate System-to-Intermediate System (IS-IS) link-state database, use the **show isis database** command in user EXEC or privileged EXEC mode.

show isis [*area-tag*] **database** [**level-1**] [**level-2**] [**I1**] [**I2**] [**detail**] [**lspid**]

| Syntax Description | | |
|--------------------|--|---|
| <i>area-tag</i> | | (Optional) Meaningful name for a routing process. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. If an area tag is not specified, a null tag is assumed and the process is referenced with a null tag. If an area tag is specified, output is limited to the specified area. |
| level-1 | | (Optional) Displays the IS-IS link-state database for Level 1. |
| level-2 | | (Optional) Displays the IS-IS link-state database for Level 2. |
| I1 | | (Optional) Abbreviation for the level-1 option. |
| I2 | | (Optional) Abbreviation for the level-2 option. |
| detail | | (Optional) When specified, displays the contents of each link-state packet (LSP). Otherwise, a summary display is provided. |
| lspid | | (Optional) When specified, displays the link-state protocol data unit (PDU) identifier. Displays the contents of a single LSP by its ID number. |

| Command Modes | User EXEC Privileged EXEC |
|---------------|------------------------------|
|---------------|------------------------------|

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 10.0 | This command was introduced. |
| | 12.2(15)T | Support was added for IPv6. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

| Usage Guidelines | The order of the optional argument and keywords is not important when entering this command. For example, the following are both valid command specifications and provide the same output: show isis database detail I2 and show isis database I2 detail . |
|------------------|--|
|------------------|--|

| Examples | The following is sample output from the show isis database command: |
|----------|--|
|----------|--|

```
Router# show isis database
```

```
IS-IS Level-1 Link State Database
LSPID          LSP Seq Num    LSP Checksum   LSP Holdtime   ATT/P/OL
0000.0C00.0C35.00-00  0x0000000C    0x5696         792            0/0/0
0000.0C00.40AF.00-00* 0x00000009    0x8452         1077           1/0/0
0000.0C00.62E6.00-00  0x0000000A    0x38E7         383            0/0/0
```

```

0000.0C00.62E6.03-00 0x00000006 0x82BC 384 0/0/0
0800.2B16.24EA.00-00 0x00001D9F 0x8864 1188 1/0/0
0800.2B16.24EA.01-00 0x00001E36 0x0935 1198 1/0/0

```

IS-IS Level-2 Link State Database

```

LSPID          LSP Seq Num    LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.03-00 0x00000005    0x04C8       792           0/0/0
0000.0C00.3E51.00-00 0x00000007    0xAF96       758           0/0/0
0000.0C00.40AF.00-00* 0x0000000A    0x3AA9       1077          0/0/0

```

Table 114 describes the significant fields shown in the display.

Table 114 show isis database Field Descriptions

| Field | Description |
|--------------|---|
| LSPID | <p>The LSP identifier. The first six octets form the system ID of the router that originated the LSP.</p> <p>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 will describe the state of the originating router.</p> <p>For each LAN, the designated router for that LAN will create and flood a pseudonode LSP, describing all systems attached to that LAN.</p> <p>The last octet is the LSP number. If there is more data than can fit in a single LSP, the LSP will be divided into multiple LSP fragments. Each fragment will have a different LSP number. An asterisk (*) indicates that the LSP was originated by the system on which this command is issued.</p> |
| 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 will stay in the LSDB before being completely removed. |
| ATT | The 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 will use the Attach bit to find the closest Level 2 router. They will point a default route to the closest Level 2 router. |
| P | The P bit. Detects if the intermediate systems is area partition repair-capable. Cisco and other vendors do not support area partition repair. |
| OL | The Overload bit. Determines if the IS is congested. If the Overload bit is set, other routers will not use this system as a transit router when calculating routes. Only packets for destinations directly connected to the overloaded router will be sent to this router. |

The following is sample output from the **show isis database detail** command:

```
Router# show isis database detail
```

```
IS-IS Level-1 Link State Database
LSPID                LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.00-00 0x0000000C  0x5696        325           0/0/0
  Area Address: 47.0004.004D.0001
  Area Address: 39.0001
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.0C35
--More--
0000.0C00.40AF.00-00* 0x00000009  0x8452        608           1/0/0
  Area Address: 47.0004.004D.0001
  Topology: IPv4 (0x0) IPv6 (0x2)
  NLPID: 0xCC 0x8E
  IP Address: 172.16.21.49
  Metric: 10   IS 0800.2B16.24EA.01
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.40AF
  IPv6 Address: 2001:0DB8::/32
  Metric: 10   IPv6 (MT-IPv6) 2001:0DB8::/64
  Metric: 5     IS-Extended cisco.03
  Metric: 10   IS-Extended cisco1.03
  Metric: 10   IS (MT-IPv6) cisco.03
```

As the output shows, in addition to the information displayed with the **show isis database** command, the **show isis database detail** command displays the contents of each LSP.

Table 115 describes the significant fields shown in the display.

Table 115 *show isis database detail Field Descriptions*

| Field | Description |
|---------------|---|
| 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. |
| 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 CLNS prefix). |
| Topology | States the topology supported (for example, IPv4, IPv6). |
| IPv6 Address | The IPv6 address. |
| MT-IPv6 | Advertised using multitopology TLV. |

The following is additional sample output from the **show isis database detail** command. This LSP is a Level 2 LSP. The area address 39.0001 is the address of the area in which the router resides.

```
Router# show isis database detail l2
```

```
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:   172.16.64.17
  Metric: 10   IS 0000.0C00.1111.09
  Metric: 10   IS 0000.0C00.1111.08
  Metric: 10   IP 172.16.65.0 255.255.255.0
```

show isis ipv6 rib

To display the IPv6 local routing information base (RIB), use the **show isis ipv6 rib** command in user EXEC or privileged EXEC mode.

show isis ipv6 rib [*ipv6-prefix*]

no show isis ipv6 rib [*ipv6-prefix*]

| | |
|---------------------------|---|
| Syntax Description | <div> <div><i>ipv6-prefix</i></div> <div>(Optional) IPv6 address prefix.</div> <div>This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</div> </div> |
|---------------------------|---|

| | |
|----------------------|---|
| Command Modes | <div>User EXEC</div> <div>Privileged EXEC</div> |
|----------------------|---|

| Command History | <table> <tr> <th data-bbox="342 879 613 913">Release</th><th data-bbox="630 879 1485 913">Modification</th></tr> <tr> <td data-bbox="342 913 613 961">12.3(4)T</td><td data-bbox="630 913 1485 961">This command was introduced.</td></tr> </table> | Release | Modification | 12.3(4)T | This command was introduced. |
|------------------------|---|---------|--------------|----------|------------------------------|
| Release | Modification | | | | |
| 12.3(4)T | This command was introduced. | | | | |

| | |
|-------------------------|--|
| Usage Guidelines | <p>When the optional <i>ipv6-prefix</i> argument is not used, the complete ISIS IPv6 RIB is displayed. When an optional IPv6 prefix is supplied, only the entry matching that prefix is displayed.</p> <p>Only the optimal paths will be installed in the master IPv6 RIB as IS-IS routes.</p> |
|-------------------------|--|

| | |
|-----------------|---|
| Examples | <p>The following example shows output from the show isis ipv6 rib command. An asterisk (*) indicates prefixes that have been installed in the master IPv6 RIB as IS-IS routes. Following each prefix is a list of all paths in order of preference, with optimal paths listed first and suboptimal paths listed after optimal paths.</p> |
|-----------------|---|

```
Router# show isis ipv6 rib
```

```
IS-IS IPv6 process "", local RIB
```

```

88:1::/64
  via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L2 metric 20 LSP [3/7]
  via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L2 metric 20 LSP [3/7]
* 1357:1::/64
  via FE80::202:7DFF:FE1A:9471/Ethernet2/1, type L2 metric 10 LSP [4/9]
* 2001:45A::/64
  via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L1 metric 20 LSP [C/6]
  via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L1 metric 20 LSP [C/6]
  via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L2 metric 20 LSP [3/7]
  via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L2 metric 20 LSP [3/7]
```

Table 116 describes the significant fields shown in the display.

Table 116 show isis ipv6 rib Field Descriptions

| Field | Description |
|-----------|--|
| * | Prefixes that have been installed in the master IPv6 RIB as IS-IS routes. |
| Type | Type of path. L1—Level 1 L2—Level 2 IA—Inter-area Sum—Summary |
| LSP [3/7] | Link-state packet (LSP). The numbers following LSP indicate the LSP index and LSP version, respectively. |

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** user command in user EXEC or privileged EXEC mode.

```
show isis [area-tag] [ipv6 | *] spf-log
```

| | | |
|--------------------|----------|--|
| Syntax Description | area-tag | (Optional) Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration. |
| | | Meaningful name for a routing process. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. If an area tag is not specified, a null tag is assumed and the process is referenced with a null tag. If an area tag is specified, output is limited to the specified area. |
| | ipv6 | (Optional) Displays IS-IS multitopology for IPv6 SPF log. |
| | * | (Optional) Displays the SPF logs of all address families. |

| | |
|---------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 10.0 | This command was introduced. |
| | 12.2(15)T | Support was added for IPv6. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Examples The following is sample output from the **show isis spf-log** command with the optional **ipv6** keyword:

```
Router# show isis ipv6 spf-log
```

| IPv6 Level 1 SPF log | | | | | |
|----------------------|----------|-------|-------|------------------|----------------------|
| When | Duration | Nodes | Count | Last trigger LSP | Triggers |
| 00:15:46 | 3124 | 40 | 1 | milles.00-00 | TLVCODE |
| 00:15:24 | 3216 | 41 | 5 | milles.00-00 | TLVCODE NEWLSP |
| 00:15:19 | 3096 | 41 | 1 | deurze.00-00 | TLVCODE |
| 00:14:54 | 3004 | 41 | 2 | milles.00-00 | ATTACHFLAG LSPHEADER |
| 00:14:49 | 3384 | 41 | 1 | milles.00-01 | TLVCODE |
| 00:14:23 | 2932 | 41 | 3 | milles.00-00 | TLVCODE |
| 00:05:18 | 3140 | 41 | 1 | | PERIODIC |
| 00:03:54 | 3144 | 41 | 1 | milles.01-00 | TLVCODE |
| 00:03:49 | 2908 | 41 | 1 | milles.01-00 | TLVCODE |
| 00:03:28 | 3148 | 41 | 3 | bakel.00-00 | TLVCODE TLVCONTENT |
| 00:03:15 | 3054 | 41 | 1 | milles.00-00 | TLVCODE |
| 00:02:53 | 2958 | 41 | 1 | mortel.00-00 | TLVCODE |
| 00:02:48 | 3632 | 41 | 2 | milles.00-00 | NEWADJ TLVCODE |
| 00:02:23 | 2988 | 41 | 1 | milles.00-01 | TLVCODE |
| 00:02:18 | 3016 | 41 | 1 | gemert.00-00 | TLVCODE |
| 00:02:14 | 2932 | 41 | 1 | bakel.00-00 | TLVCONTENT |

```

00:02:09      2988      41      2      bakel.00-00  TLVCONTENT
00:01:54      3228      41      1      milles.00-00 TLVCODE
00:01:38      3120      41      3      rips.03-00  TLVCONTENT

```

Table 117 describes the significant fields shown in the display.

Table 117 *show isis spf-log Field Descriptions*

| Field | Description |
|------------------|---|
| When | How long ago (in hours: minutes: seconds) a full SPF calculation occurred. The last 20 occurrences are logged. |
| Duration | Number of milliseconds required 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. |
| 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. A router waits 5 seconds before running a full SPF run, 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 SPF. |
| Last trigger LSP | Whenever a full SPF calculation is triggered by the arrival of a new LSP, the router stores the LSP ID. The LSP ID can provide a clue as to the source of routing instability in an area. If multiple LSPs are causing an SPF run, only the LSP ID of the last received LSP is remembered. |
| Triggers | A list of all reasons that triggered a full SPF calculation. For a list of possible triggers, see Table 29. |

Table 118 lists possible triggers of a full SPF calculation.

Table 118 *Possible Triggers of Full SPF Calculation*

| Trigger | Description |
|------------|--|
| ATTACHFLAG | This router is now attached to the Level 2 backbone or it has just lost contact to the Level 2 backbone. |
| ADMINDIST | Another administrative distance was configured for the IS-IS process on this router. |
| AREASET | Set of learned area addresses in this area changed. |
| BACKUPOVFL | An IP prefix disappeared. The router knows there is another way to reach that prefix but has not stored that backup route. The only way to find the alternative route is through a full SPF run. |
| DBCHANGED | A clear isis * command was issued on this router. |
| IPBACKUP | An IP route disappeared, which was not learned via IS-IS, but via another protocol with better administrative distance. IS-IS will run a full SPF to install an IS-IS route for the disappeared IP prefix. |
| IPQUERY | A clear ip route command was issued on this router. |
| LSPEXPIRED | Some LSP in the link-state database (LSDB) has expired. |

Table 118 Possible Triggers of Full SPF Calculation (continued)

| Trigger | Description |
|------------|--|
| LSPHEADER | ATT/P/OL bits or is-type in an LSP header changed. |
| NEWADJ | This router has created a new adjacency to another router. |
| NEWAREA | A new area (via network entity title [NET]) was configured on this router. |
| NEWLEVEL | A new level (via is-type) was configured on this router. |
| NEWLSP | A new router or pseudonode appeared in the topology. |
| NEWMETRIC | A new metric was configured on an interface of this router. |
| NEWSYSID | A new system ID (via NET) was configured on this router. |
| PERIODIC | Typically, every 15 minutes a router runs a periodic full SPF calculation. |
| RTCLEARED | A clear cls route command was issued on this router. |
| TLVCODE | TLV code mismatch, indicating that different TLVs are included in the newest version of an LSP. |
| TLVCONTENT | TLV contents changed. This normally indicates that an adjacency somewhere in the area has come up or gone down. The “Last trigger LSP” column indicates where the instability may have occurred. |

show isis topology

To display a list of all connected routers in all areas, use the **show isis topology** command in user EXEC or privileged EXEC mode.

show isis [*area-tag*] [**ipv6** | *] **topology**

| | | |
|---------------------------|-----------------|---|
| Syntax Description | <i>area-tag</i> | (Optional) Meaningful name for a routing process. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. If an area tag is not specified, a null tag is assumed and the process is referenced with a null tag. If an area tag is specified, output is limited to the specified area. |
| | ipv6 | (Optional) Displays IS-IS IPv6 topology. |
| | * | (Optional) Displays the topology of all address families. |

| | |
|----------------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.0(5)T | This command was introduced. |
| | 12.2(15)T | Support was added for IPv6. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

| | |
|-------------------------|--|
| Usage Guidelines | Use the show isis topology EXEC command to verify the presence and connectivity between all routers in all areas. |
|-------------------------|--|

| | |
|-----------------|---|
| Examples | The following example shows output from the show isis topology command using the optional IPv6 keyword. The command shown used in a dual CLNS-IP network: |
|-----------------|---|

```
Router# show isis ipv6 topology
```

```
Area L2BB:
IS-IS IPv6 paths to level-1 routers
System Id      Metric  Next-Hop      Interface      SNPA
0000.0000.0005 --
0000.0000.0009 10      0000.0000.0009 Tu529          *Tunnel*
0000.0000.0017 20      0000.0000.0009 Tu529          *Tunnel*
0000.0000.0053 30      0000.0000.0009 Tu529          *Tunnel*
0000.0000.0068 20      0000.0000.0009 Tu529          *Tunnel*

IS-IS paths to level-2 routers
System Id      Metric  Next-Hop      Interface      SNPA
0000.0000.0005 --
0000.0000.0009 10      0000.0000.0009 Tu529          *Tunnel*
0000.0000.0017 20      0000.0000.0009 Tu529          *Tunnel*
```

```

0000.0000.0053 30      0000.0000.0009 Tu529      *Tunnel*
0000.0000.0068 20      0000.0000.0009 Tu529      *Tunnel*
Area A3253-01:
IS-IS paths to level-1 routers
System Id      Metric  Next-Hop      Interface     SNPA
0000.0000.0003 10      0000.0000.0003 Et1           0000.0c03.6944
0000.0000.0005 --
0000.0000.0053 10      0000.0000.0053 Et1           0060.3e58.ccdB

Area A3253-02:
IS-IS paths to level-1 routers
System Id      Metric  Next-Hop      Interface     SNPA
0000.0000.0002 10      0000.0000.0002 Et2           0000.0c03.6bc5
0000.0000.0005 --
0000.0000.0053 10      0000.0000.0053 Et2           0060.3e58.ccde

```

Table 119 describes the significant fields shown in the display.

Table 119 *show isis topology Field Descriptions*

| Field | Description |
|-----------|---|
| Area | Identifies the routing process. |
| System Id | Six-byte value that identifies a system in an area. |
| 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 CLNS prefix). |
| Next-Hop | The address of the next hop router. |
| Interface | Interface from which the system was learned. |
| SNPA | Subnetwork point of attachment. This is the data-link address. |

show mpls forwarding-table

To display the contents of the Multiprotocol Label Switching (MPLS) label forwarding information base (LFIB), use the **show mpls forwarding-table** command in user EXEC mode.

```
show mpls forwarding-table [network {mask | length} | destination-ipv6-prefix | labels label
[- label] | interface interface | next-hop address | lsp-tunnel [tunnel-id] ] [vrf vrf-name]
[detail]
```

| Syntax Description | |
|------------------------------------|--|
| <i>network</i> | (Optional) Destination network number. |
| <i>mask</i> | (Optional) IP address of the destination mask whose entry is to be shown. |
| <i>length</i> | (Optional) Number of bits in mask of destination. |
| <i>destination-ipv6-prefix</i> | The destination IPv6 network or class of networks. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| labels <i>label - label</i> | (Optional) Displays only entries with the specified local labels. |
| interface <i>interface</i> | (Optional) Displays only entries with the specified outgoing interface. |
| next-hop <i>address</i> | (Optional) Displays only entries with the specified neighbor as the next hop. |
| lsp-tunnel <i>tunnel-id</i> | (Optional) Displays only entries with the specified label switched path (LSP) tunnel, or with all LSP tunnel entries. |
| vrf <i>vrf-name</i> | (Optional) Displays only entries with the specified VPN routing/forwarding instance (VRF). |
| detail | (Optional) Displays information in long form (includes length of encapsulation, length of MAC string, maximum transmission unit (MTU), and all labels). |

Command Modes User EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 11.1 CT | This command was introduced. |
| | 12.1(3)T | This command was modified to reflect new MPLS Internet Engineering Task Force (IETF) terminology and command-line interface (CLI) command syntax. |
| | 12.2(8)T | The command was modified to accommodate use of the MPLS experimental (EXP) level as a selection criteria for packet forwarding. The output display was modified to include a bundle adjacency field and exp (vcd) values when the optional detail keyword is specified. |
| | 12.0(22)S | IPv6 MPLS aggregate label and prefix information was added to the display. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| | 12.3(2)T | Modified IPv6 MPLS aggregate label and prefix information was added to the display. IPv6 prefixes are now supported. |

Usage Guidelines

The options described allow specification of a subset of the entire LFIB.

Examples**Basic Command Output**

The following is sample output from the **show mpls forwarding-table** command:

```
Router# show mpls forwarding-table
```

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop |
|-----------|--------------------|---------------------|--------------------|--------------------|-------------|
| 26 | Untagged | 10.253.0.0/16 | 0 | Et4/0/0 | 172.27.32.4 |
| 28 | 1/33 | 10.15.0.0/16 | 0 | AT0/0.1 | point2point |
| 29 | Pop tag | 10.91.0.0/16 | 0 | Hs5/0 | point2point |
| | 1/36 | 10.91.0.0/16 | 0 | AT0/0.1 | point2point |
| 30 | 32 | 10.250.0.97/32 | 0 | Et4/0/2 | 10.92.0.7 |
| | 32 | 10.250.0.97/32 | 0 | Hs5/0 | point2point |
| 34 | 26 | 10.77.0.0/24 | 0 | Et4/0/2 | 10.92.0.7 |
| | 26 | 10.77.0.0/24 | 0 | Hs5/0 | point2point |
| 35 | Untagged [T] | 10.100.100.101/32 | 0 | Tu301 | point2point |
| 36 | Pop tag | 168.1.0.0/16 | 0 | Hs5/0 | point2point |
| | 1/37 | 168.1.0.0/16 | 0 | AT0/0.1 | point2point |

[T] Forwarding through a TSP tunnel.
View additional tagging info with the 'detail' option

IPv6 Provider Edge Router over MPLS

The following is sample output from the **show mpls forwarding-table** command when the IPv6 Provider Edge Router over MPLS feature is configured to allow IPv6 traffic to be transported across an IPv4 MPLS backbone. The labels are aggregate because there are several prefixes for one local label, and the prefix column contains “IPv6” instead of a target prefix.

```
router# show mpls forwarding-table
```

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop |
|-----------|--------------------|---------------------|--------------------|--------------------|-------------|
| 16 | Pop tag | 70.1.1.0/24 | 0 | Se1/0 | point2point |
| 17 | Pop tag | 70.1.1.0/24 | 0 | Se1/0 | point2point |
| 18 | 19 | 70.1.0.0/16 | 0 | Se1/0 | point2point |
| 19 | Pop tag | 5001::/64 | 520 | Se1/0 | point2point |
| 20 | 21 | 90.90.90.1/32 | 0 | Se1/0 | point2point |
| 21 | Pop tag | 60.1.0.0/16 | 0 | Se1/0 | point2point |
| 22 | 20 | 80.1.0.0/16 | 0 | Se1/0 | point2point |
| 26 | Aggregate | 4000::/48 | 1040 | | |

Command Output Using the detail Keyword

The following is sample output from the **show mpls forwarding-table** command when you specify the **detail** keyword. If the MPLS EXP level is used as a selection criterion for packet forwarding, a Bundle adjacency exp (vcd) field is included in the display. This field includes the EXP value and the corresponding virtual circuit descriptor (VCD) in parentheses:

```
Router# show mpls forwarding-table detail
```

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop |
|---|--------------------|---------------------|--------------------|--------------------|-------------|
| 16 | Pop tag | 1.0.0.6/32 | 0 | AT1/0.1 | point2point |
| Bundle adjacency exp(vcd) | | | | | |
| 0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1) | | | | | |
| MAC/Encaps=12/12, MTU=4474, Tag Stack{} | | | | | |

```

00010000AAAA0300000008847
No output feature configured
17 18      1.0.0.9/32      0      AT1/0.1      point2point
Bundle adjacency exp(vcd)
0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
MAC/Encaps=12/16, MTU=4470, Tag Stack{18}
00010000AAAA0300000008847 00012000
No output feature configured
18 19      1.0.0.10/32     0      AT1/0.1      point2point
Bundle adjacency exp(vcd)
0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
MAC/Encaps=12/16, MTU=4470, Tag Stack{19}
00010000AAAA0300000008847 00013000
No output feature configured
19 17      20.0.0.0/8      0      AT1/0.1      point2point
Bundle adjacency exp(vcd)
0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
MAC/Encaps=12/16, MTU=4470, Tag Stack{17}
00010000AAAA0300000008847 00011000
No output feature configured
20 20      60.0.0.0/8      0      AT1/0.1      point2point
Bundle adjacency exp(vcd)
0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
MAC/Encaps=12/16, MTU=4470, Tag Stack{20}
00010000AAAA0300000008847 00014000
No output feature configured
21 Pop tag      60.0.0.0/24      0      AT1/0.1      point2point
Bundle adjacency exp(vcd)
0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
MAC/Encaps=12/12, MTU=4474, Tag Stack{}
00010000AAAA0300000008847
No output feature configured
22 Pop tag      1.0.0.4/32      0      Et2/3      40.0.0.4
MAC/Encaps=14/14, MTU=1504, Tag Stack{}
000427AD10430005DDFE043B8847
No output feature configured

```

Table 120 describes the significant fields shown in the displays.

Table 120 *show mpls forwarding-table Field Descriptions*

| Field | Description |
|------------------------------------|--|
| Local tag | Label assigned by this router. Local tag 19 (pop tag) label allows fast MPLS switching on interface Se1/0. |
| Outgoing tag or VC | Label assigned by the next hop or virtual path identifier (VPI)/virtual channel identifier (VCI) used to get to next hop. The entries that you can specify in this column include the following: <ul style="list-style-type: none"> • [T]—Means forwarding through an LSP tunnel. • “Untagged”—Means that there is no label for the destination from the next hop or that label switching is not enabled on the outgoing interface. • “Pop tag”—Means that the next hop advertised an implicit NULL label for the destination and that this router popped the top label. • “Aggregate”—Means there are several prefixes for one local label. Used when IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network. |
| Prefix or Tunnel Id | Address or tunnel to which packets with this label are going. Note If IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network, “IPv6” is displayed here. |
| Bytes tag switched | Number of bytes switched with this incoming label. |
| Outgoing interface | Interface through which packets with this label are sent. |
| Next Hop | IP address of the neighbor that assigned the outgoing label. |
| Bundle adjacency exp (vcd) | Bundle adjacency information. Includes the MPLS EXP value and the corresponding VCD. |
| MAC/Encaps | Length in bytes of the Layer 2 header and length in bytes of the packet encapsulation, including the Layer 2 header and label header. |
| MTU | Maximum transmission unit (MTU) of the labeled packet. |
| Tag Stack | All the outgoing labels. If the outgoing interface is transmission convergence (TC)-ATM, the VCD is also shown. |
| 00010000AAAA0300000008847 00013000 | The actual encapsulation in hexadecimal form. A space is shown between Layer 2 and the label header. |

spf-interval (IPv6)

To configure how often Cisco IOS software performs the shortest path first (SPF) calculation, use the **spf-interval** command in address family configuration mode. To restore the default interval, use the **no** form of this command.

spf-interval [**level-1** | **level-2**] *seconds* [*initial-wait*] [*secondary-wait*]

no spf-interval *seconds*

| | | |
|---------------------------|-----------------------|--|
| Syntax Description | level-1 | (Optional) Summarizes only routes redistributed into Level 1 with the configured prefix value. |
| | level-2 | (Optional) Summarizes routes learned by Level 1 routing into the Level 2 backbone with the configured prefix value. Redistributed routes into Level 2 IS-IS also are summarized. |
| | <i>seconds</i> | Minimum amount of time between SPF calculations, in seconds. It can be a number from 1 to 120. The default is 5 seconds. |
| | <i>initial-wait</i> | (Optional) Length of time before the first SPF calculation in milliseconds. |
| | <i>secondary-wait</i> | (Optional) Minimum length of time between the first and second SPF calculation, in milliseconds. |
| | | |

Defaults 5 seconds

Command Modes Address family configuration

| Command History | Release | Modification |
|------------------------|----------------|---|
| | 12.2(15)T | This command was introduced. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |
| | 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S. |

Usage Guidelines SPF calculations are performed only when the topology changes. They are not performed when external routes change.

The **spf-interval** (IPv6) command controls how often Cisco IOS software can perform the SPF calculation. The SPF calculation is processor-intensive. Therefore, it may be useful to limit how often the SPF calculation is performed, especially when the area is large and the topology changes often. Increasing the SPF interval reduces the processor load of the router, but it could slow down the rate of convergence.

If IPv6 and IPv4 are configured on the same interface, they must be running the same Intermediate System-to-Intermediate System (IS-IS) level.

You can use the **spf-interval** (IPv6) command only when using the IS-IS multitopology support for IPv6 feature.

Examples

The following example sets the SPF calculation interval to 30 seconds:

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# spf-interval 30
```

Related Commands

| Command | Description |
|---------------------|---|
| prc-interval (IPv6) | Controls the hold-down period between PRCs. |

split-horizon (IPv6 RIP)

To configure split horizon processing of IPv6 Routing Information Protocol (RIP) router updates, use the **split-horizon** command in router configuration mode. To disable the split horizon processing of IPv6 RIP updates, use the **no** form of this command.

split-horizon

no split-horizon

Syntax Description This command has no keywords or arguments.

Defaults Split horizon is configured.

Command Modes Router configuration

| Command History | Release | Modification |
|-----------------|------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines The **split-horizon** (IPv6 RIP) command is similar to the **ip split-horizon** command, except that it is IPv6-specific.

This command configures split horizon processing of IPv6 RIP router updates. When split horizon is configured, the advertisement of networks out the interfaces from which the networks are learned is suppressed.

If both split horizon and poison reverse are configured, then split horizon behavior is replaced by poison reverse behavior (routes learned via RIP are advertised out the interface over which they were learned, but with an unreachable metric).



Note

In general, changing the state of the default for the **split-horizon** command is not recommended, unless you are certain that your application requires a change in order to properly advertise routes. If split horizon is disabled on a serial interface (and that interface is attached to a packet-switched network), you *must* disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Examples The following example configures split horizon processing for the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
```

Router(config-rtr-rip)# **split-horizon**

| Related Commands | Command | Description |
|------------------|-----------------------|--|
| | neighbor (RIP) | Defines a neighboring router with which to exchange routing information. |

ssh

To start an encrypted session with a remote networking device, use the **ssh** command in user EXEC mode.

```
ssh [-l userid] [-c {des | 3des}] [-o numberofpasswdprompts n] [-p portnum] {address | hostname}  
[command]
```

| Syntax Description | | |
|---|------------|--|
| -l <i>userid</i> | (Optional) | Specifies the user ID to use when logging in as on the remote networking device running the SSH server. If no user ID is specified, the default is the current user ID. |
| -c { des 3des } | (Optional) | Specifies the crypto algorithm, DES or 3DES, to use for encrypting data. To use SSH, you must have an encryption image running on the router. Cisco software images that include encryption have the designator “k8” (DES) or “k9” (3DES). |
| -o numberofpasswdprompts <i>n</i> | (Optional) | Specifies the number of password prompts that the software generates before ending the session. The SSH server may also apply a limit to the number of attempts. If the limit set by the server is less than the value specified by the -o numberofpasswdprompts keyword, the limit set by the server takes precedence. The default is three attempts, which is also the Cisco IOS SSH server default. The range of values is from 1 to 5. |
| -p <i>portnum</i> | (Optional) | Indicates the desired port number for the remote host. The default port number is 22. |
| <i>address</i> <i>hostname</i> | | Specifies the IPv4 or IPv6 address, or host name of the remote networking device. |
| <i>command</i> | (Optional) | Specifies the Cisco IOS command that you want to run on the remote networking device. If the remote host is not running Cisco IOS software, this may be any command recognized by the remote host. If the command includes spaces, you must enclose the command in quotation marks. |

| | |
|-----------------|----------|
| Defaults | Disabled |
|-----------------|----------|

| | |
|----------------------|-----------|
| Command Modes | User EXEC |
|----------------------|-----------|

| Command History | Release | Modification |
|-----------------|--|---------------------------------------|
| | 12.1(3)T | This command was introduced. |
| | 12.2(8)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S | Support for IPv6 addresses was added. |

Usage Guidelines

The **ssh** command enables a Cisco router to make a secure, encrypted connection to another Cisco router or device running an SSH Version 1 server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.



Note

SSH is supported on DES (56-bit) and 3DES (168-bit) data encryption software images only. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.

The **ssh** command requires that you first enable the SSH server on the router. The SSH client is available only when the SSH server is enabled.

Examples

The following example illustrates initiating a secure session between the local router and the remote host HQhost to run the **show users** command. The result of the **show users** command is a list of valid users that are logged in to HQhost. The remote host will prompt for the adminHQ password to authenticate the user adminHQ. If the authentication step is successful, the remote host will return the result of the **show users** command to the local router and will then close the session.

```
ssh -l adminHQ HQhost "show users"
```

The following example illustrates initiating a secure session between the local router and the edge router HQedge to run the **show ip route** command. In this example, the edge router prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the edge router will return the result of the **show ip route** command to the local router and will then close the session.

```
ssh -l adminHQ HQedge "show ip route"
```

The following example shows the SSH client using 3DES to initiate a secure remote command connection with the HQedge router. The SSH server running on HQedge authenticates the session for the admin7 user on the HQedge router using standard authentication methods. The HQedge router must have SSH enabled for authentication to work.

```
ssh -l admin7 -c 3des -o numberofpasswdprompts 5 HQedge
```

The following example shows a secure session between the local router and a remote IPv6 router with the address 2001:0DB8:2222::72 to run the **show running-config** command. In this example, the remote IPv6 router prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the remote IPv6 router will return the result of the **show running-config** command to the local router and will then close the session.

```
ssh -l adminHQ 2001:0DB8:2222::72 "show running-config"
```



Note

A host name that maps to the IPv6 address 2001:0DB8:2222::72 could have been used in the last example.

Related Commands

| Command | Description |
|--------------------|---|
| ip ssh | Configures SSH server control parameters on the router. |
| show ip ssh | Displays the version and configuration data for SSH. |
| show ssh | Displays the status of SSH server connections. |

summary-prefix (IPv6 IS-IS)

To create aggregate IPv6 prefixes for Intermediate System-to-Intermediate System (IS-IS), use the **summary-prefix** command in address family configuration mode. To restore the default, use the **no** form of this command.

summary-prefix *ipv6-prefix/prefix-length* {**level-1** | **level-1-2** | **level-2**}

no summary-prefix *ipv6-prefix/prefix-length* {**level-1** | **level-1-2** | **level-2**}

| | | |
|---------------------------|-----------------------|--|
| Syntax Description | <i>ipv6-prefix</i> | Summary prefix designated for a range of IPv6 prefixes. The <i>ipv6-prefix</i> 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> | The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |
| | level-1 | Only routes redistributed into Level 1 are summarized with the configured prefix value. |
| | level-1-2 | Summary routes are applied when redistributing routes into Level 1 and Level 2 IS-IS, and when Level 2 IS-IS advertises Level 1 routes reachable in its area. |
| | level-2 | Routes learned by Level 1 routing are summarized into the Level 2 backbone with the configured prefix value. Redistributed routes into Level 2 IS-IS will be summarized also. |

Defaults All redistributed routes are advertised individually.

Command Modes Address family configuration

| | | |
|------------------------|----------------|--|
| Command History | Release | Modification |
| | 12.2(8)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines Multiple groups of prefixes 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. This command helps reduce the size of the routing updates generated by the router, resulting in smaller routing tables on neighbor routers.

This command also reduces the size of the link-state packets (LSPs) and thus the link-state database (LSDB). It also helps ensure stability because a summary advertisement is depending on many more specific routes. If one more specific route flaps, in most cases this flapping does not cause a flap of the summary advertisement.

The drawback of summary prefixes is that other routes might have less information with which 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 IPv6 routing table but labels it as a “discard” route entry. Any packet that matches the entry will be discarded to prevent routing loops. When IS-IS stops advertising the summary prefix, the routing table entry is removed.

Examples

The following example redistributes Routing Information Protocol (RIP) routes into IS-IS. In the RIP routing table, there are IPv6 routes for 3FFE:F000:0001:0000::/64, 3FFE:F000:0002:0000::/64, 3FFE:F000:0003:0000::/64, and so on. This example advertises only 3FFE:F000::/24 into IPv6 IS-IS Level 1.

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6
Router(config-router-af)# redistribute rip level-1 metric 40
Router(config-router-af)# summary-prefix 3FFE:F000::/24 level-1
```

summary-prefix (IPv6 OSPF)

To configure an IPv6 summary prefix, use the **summary-prefix** command in router configuration mode. To restore the default, use the **no** form of this command.

summary-prefix *prefix* [**not-advertise** | **tag** *tag-value*]

no summary-prefix *prefix* [**not-advertise** | **tag** *tag-value*]

| | | |
|---------------------------|-----------------------------|--|
| Syntax Description | <i>prefix</i> | IPv6 route prefix for the destination. |
| | not-advertise | (Optional) Suppress routes that match the specified prefix and mask pair. This keyword applies to OSPF only. |
| | tag <i>tag-value</i> | (Optional) Tag value that can be used as a “match” value for controlling redistribution via route maps. This keyword applies to OSPF only. |

Defaults No IPv6 summary prefix is defined.

Command Modes Router configuration

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.0(24)S | This command was introduced. |
| | 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. |
| | 12.2(18)S | This command was integrated into Cisco IOS Release 12.2(18)S. |

Usage Guidelines This command can be used to summarize routes redistributed from other routing protocols. Multiple groups of addresses can be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing table.

Examples In the following example, the summary prefix FEC0::/24 includes addresses FEC0::/1 through FEC0::/24. Only the address FEC0::/24 is advertised in an external link-state advertisement.

```
ipv6 router ospf 1
router-id 172.16.3.3
summary-prefix FEC0::/24
redistribute static
```

synchronization (IPv6)

To enable the synchronization between IPv6 Border Gateway Protocol (BGP) and your Interior Gateway Protocol (IGP) system, use the **synchronization** command in address family configuration mode. To enable the Cisco IOS software to advertise a network route without waiting for IGP, use the **no** form of this command.

synchronization

no synchronization

Syntax Description This command has no arguments or keywords.

Defaults BGP advertises network routes without waiting for IGP.

Command Modes Address family configuration

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.2(8)T | This command was introduced. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines Unlike the IPv4 version of the **synchronization** command, the IPv6 version is disabled by default.

By default, an IPv6 BGP speaker advertises an IPv6 network route without waiting for the IGP. Use the **synchronization** command in address family configuration mode to synchronize routing advertisements between BGP and your IGP. This feature allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems. When synchronization is enabled, IPv6 BGP does not advertise a route to an external neighbor unless that route is local or exists in the IGP.

Use the **synchronization** command if routers in the autonomous system do not speak BGP.

Examples The following example enables a router to advertise an IPv6 network route without waiting for an IGP:

```
router bgp 65000
address-family ipv6
 synchronization
```


telnet

To log in to a host that supports Telnet, use the **telnet** command in user EXEC or privileged EXEC mode.

telnet *host* [*port*] [*keyword*]

| | | |
|---------------------------|----------------|---|
| Syntax Description | <i>host</i> | A host name or an IP address. |
| | <i>port</i> | (Optional) A decimal TCP port number, or port name; the default is the Telnet router port (decimal 23) on the host. |
| | <i>keyword</i> | (Optional) One of the keywords listed in Table 121. |

| | |
|----------------------|-----------------|
| Command Modes | User EXEC |
| | Privileged EXEC |

| | | |
|------------------------|--|--------------------------------------|
| Command History | Release | Modification |
| | 10.0 | This command was introduced. |
| | 12.1 | The /quiet keyword was added. |
| | 12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S | The /ipv6 keyword was added. |
| | | |

| | |
|-------------------------|--|
| Usage Guidelines | Table 121 lists the optional telnet command keywords. |
|-------------------------|--|

Table 121 telnet Keyword Options

| Option | Description |
|------------------------------|--|
| /debug | Enables Telnet debugging mode. |
| /encrypt kerberos | Enables an encrypted Telnet session. This keyword is available only if you have the Kerberized Telnet subsystem. If you authenticate using Kerberos Credentials, the use of this keyword initiates an encryption negotiation with the remote server. If the encryption negotiation fails, the Telnet connection will be reset. If the encryption negotiation is successful, the Telnet connection will be established, and the Telnet session will continue in encrypted mode (all Telnet traffic for the session will be encrypted). |
| /ipv4 | Specifies version 4 of the IP protocol. If a version of the IP protocol is not specified in a network that supports both the IPv4 and IPv6 protocol stacks, IPv6 is attempted first and is followed by IPv4. |
| /ipv6 | Specifies version 6 of the IP protocol. If a version of the IP protocol is not specified in a network that supports both the IPv4 and IPv6 protocol stacks, IPv6 is attempted first and is followed by IPv4. |

Table 121 telnet Keyword Options (continued)

| Option | Description |
|--------------------------|--|
| /line | Enables Telnet line mode. In this mode, the Cisco IOS software sends no data to the host until you press the Enter key. You can edit the line using the standard Cisco IOS software command-editing characters. The /line keyword is a local switch; the remote router is not notified of the mode change. |
| /noecho | Disables local echo. |
| /quiet | Prevents onscreen display of all messages from the Cisco IOS software. |
| /route: path | Specifies loose source routing. The <i>path</i> argument is a list of host names or IP addresses that specify network nodes and ends with the final destination. |
| /source-interface | Specifies the source interface. |
| /stream | Turns on <i>stream</i> processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols. |
| <i>port-number</i> | Port number. |
| bgp | Border Gateway Protocol. |
| chargen | Character generator. |
| cmd rcmd | Remote commands. |
| daytime | Daytime. |
| discard | Discard. |
| domain | Domain Name Service. |
| echo | Echo. |
| exec | EXEC. |
| finger | Finger. |
| ftp | File Transfer Protocol. |
| ftp-data | FTP data connections (used infrequently). |
| gopher | Gopher. |
| hostname | Host name server. |
| ident | Ident Protocol. |
| irc | Internet Relay Chat. |
| klogin | Kerberos login. |
| kshell | Kerberos shell. |
| login | Login (rlogin). |
| lpd | Printer service. |
| nntp | Network News Transport Protocol. |
| pim-auto-rp | Protocol Independent Multicast (PIM) auto-rendezvous point (RP). |
| node | Connect to a specific Local-Area Transport (LAT) node. |
| pop2 | Post Office Protocol v2. |
| pop3 | Post Office Protocol v3. |

Table 121 telnet Keyword Options (continued)

| Option | Description |
|---------------|---|
| port | Destination local-area transport (LAT) port name. |
| smtp | Simple Mail Transfer Protocol. |
| sunrpc | Sun Remote Procedure Call. |
| syslog | Syslog. |
| tacacs | Specifies TACACS security. |
| talk | Talk (517). |
| telnet | Telnet (23). |
| time | Time (37). |
| uucp | UNIX-to-UNIX Copy Program (540). |
| whois | Nickname (43). |
| www | World Wide Web (HTTP, 80). |

With the Cisco IOS implementation of TCP/IP, you are not required to enter the **connect** or **telnet** command to establish a terminal connection. You can enter only the learned host name—as long as the following conditions are met:

- The host name is different from a command word for the router.
- The preferred transport protocol is set to **telnet**.

To display a list of the available hosts, use the **show hosts** command. To display the status of all TCP connections, use the **show tcp** command.

The Cisco IOS software assigns a logical name to each connection, and several commands use these names to identify connections. The logical name is the same as the host name, unless that name is already in use, or you change the connection name with the **name-connection EXEC** command. If the name is already in use, the Cisco IOS software assigns a null name to the connection.

The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter the escape sequence and then a command character. The default escape sequence is Ctrl-^ (press and hold the Ctrl and Shift keys and the 6 key). You can enter the command character as you hold down Ctrl or with Ctrl released; you can use either uppercase or lowercase letters. Table 122 lists the special Telnet escape sequences.

Table 122 Special Telnet Escape Sequences

| Escape Sequence ¹ | Purpose |
|------------------------------|---------------------------------|
| Ctrl-^ b | Break |
| Ctrl-^ c | Interrupt Process (IP and IPv6) |
| Ctrl-^ h | Erase Character (EC) |
| Ctrl-^ o | Abort Output (AO) |
| Ctrl-^ t | Are You There? (AYT) |
| Ctrl-^ u | Erase Line (EL) |

1. The caret (^) symbol refers to Shift-6 on your keyboard.

At any time during an active Telnet session, you can list the Telnet commands by pressing the escape sequence keys followed by a question mark at the system prompt:

Ctrl-^ ?

A sample of this list follows. In this sample output, the first caret (^) symbol represents the Ctrl key, and the second caret represents Shift-6 on your keyboard:

```
router> ^^?
[Special telnet escape help]
^^B  sends telnet BREAK
^^C  sends telnet IP
^^H  sends telnet EC
^^O  sends telnet AO
^^T  sends telnet AYT
^^U  sends telnet EL
```

You can have several concurrent Telnet sessions open and switch between them. To open a subsequent session, first suspend the current connection by pressing the escape sequence (Ctrl-Shift-6 then x [Ctrl^x] by default) to return to the system command prompt. Then open a new connection with the **telnet** command.

To terminate an active Telnet session, enter any of the following commands at the prompt of the device to which you are connecting:

- **close**
- **disconnect**
- **exit**
- **logout**
- **quit**

Examples

The following example establishes an encrypted Telnet session from a router to a remote host named *host1*:

```
router> telnet host1 /encrypt kerberos
```

The following example routes packets from the source system *host1* to *kl.sri.com*, then to *10.1.0.11*, and finally back to *host1*:

```
router> telnet host1 /route:kl.sri.com 10.1.0.11 host1
```

The following example connects to a host with the logical name *host1*:

```
router> host1
```

The following example suppresses all onscreen messages from the Cisco IOS software during login and logout:

```
router> telnet host2 /quiet
```

The following example shows the limited messages displayed when connection is made using the optional **/quiet** keyword:

```
login:User2
Password:
      Welcome to OpenVMS VAX version V6.1 on node CRAW
      Last interactive login on Tuesday, 15-DEC-1998 11:01
      Last non-interactive login on Sunday,  3-JAN-1999 22:32
```

```
Server3)logout
  User2      logged out at  16-FEB-2000 09:38:27.85
```

Related Commands

| Command | Description |
|-----------------------------------|--|
| connect | Logs in to a host that supports Telnet, rlogin, or LAT. |
| kerberos clients mandatory | Causes the rsh , rcp , rlogin , and telnet commands to fail if they cannot negotiate the Kerberos Protocol with the remote server. |
| rlogin | Logs in to a UNIX host using rlogin. |

timers (IPv6 RIP)

To configure update, timeout, hold-down, and garbage-collection timers for an IPv6 RIP routing process, use the **timers** command in router configuration mode. To return the timers to their default values, use the **no** form of this command.

timers *update timeout holddown garbage-collection*

no timers

| Syntax Description | | |
|---------------------------|--|--|
| <i>update</i> | | Interval of time (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol. |
| <i>timeout</i> | | Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the <i>update</i> argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters a hold-down state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. |
| <i>holddown</i> | | Interval (in seconds) during which routing information regarding better paths is suppressed. A route enters a hold-down state when it becomes unreachable and the hold-down timer is a value other than zero. (A learned RIP route becomes unreachable when the route is not refreshed or the route is advertised with a metric of 16.) While in hold-down state, the system ignores any new information about the route from RIP or from any protocols that have a worse administrative distance than RIP. A route with a better administrative distance will replace the unreachable route, even if the route is still in a hold-down state. |
| <i>garbage-collection</i> | | Amount of time (in seconds) that must pass from when a route becomes invalid until the route is removed from the routing table. |

| Defaults | |
|----------|---------------------------------------|
| | Update timer: 30 seconds |
| | Timeout timer: 180 seconds |
| | Hold-down timer: 0 seconds |
| | Garbage-collection timer: 120 seconds |

| Command Modes | |
|---------------|----------------------|
| | Router configuration |

| Command History | Release | Modification |
|-----------------|------------|---|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S, and the hold-down timer default value was changed to 0 seconds. |
| | 12.2(13)T | The modification to change the hold-down timer default value to 0 seconds was integrated into this release. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **timers** (IPv6 RIP) command is similar to the **timers basic** (RIP) command, except that it is IPv6-specific.

Use the *update* argument to set the time interval between RIP routing updates. If no route update is received for the time interval specified by the *timeout* argument, the route is considered unreachable. Use the *holddown* argument to set a time delay between the route becoming unreachable and the route being considered invalid in the routing table. The use of a hold-down interval is not recommended for RIP because it can introduce long delays in convergence. Use the *garbage-collection* argument to specify the time interval between a route being considered invalid and the route being purged from the routing table.

The basic timing parameters for IPv6 RIP are adjustable. Because IPv6 RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routers and access servers in the network.

**Note**

The current and default timer values are displayed in the output of the **show ipv6 rip EXEC** command. The relationships of the various timers should be preserved, as described previously.

Examples

The following example sets updates to be broadcast every 5 seconds. If a route is not heard from in 15 seconds, the route is declared unusable. Further information is suppressed for an additional 10 seconds. Assuming no updates, the route is flushed from the routing table 20 seconds after the end of the hold-down period.

```
Router(config)# ipv6 router rip cisco
Router(config-rtr-rip)# timers 5 15 10 30
```

**Caution**

By setting a short update period, you run the risk of congesting slow-speed serial lines. Also, if you have many routes in your updates, you can cause the routers to spend an excessive amount of time processing updates.

Related Commands

| Command | Description |
|----------------------|--|
| show ipv6 rip | Displays information about current IPv6 RIP processes. |

tracert

To discover the routes that packets will actually take when traveling to their destination, use the **tracert** command in user EXEC or privileged EXEC mode.

tracert [*protocol*] *destination*

Syntax Description

| | |
|--------------------|---|
| <i>protocol</i> | (Optional) Protocol keyword, either appletalk , clns , ip , ipv6 , ipx , oldvines , or vines . When not specified, the <i>protocol</i> argument is based on an examination of the format of the <i>destination</i> argument. |
| <i>destination</i> | (Optional in privileged EXEC mode; required in user EXEC mode) Destination address or host name of the system to trace. The default parameters for the appropriate protocol are assumed and the tracing action begins. |

Defaults

When not specified, the protocol argument is determined by examining the format of the *destination* argument. For example, if the software finds a *destination* argument in IP format, the protocol value defaults to IP.

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|---------------------------------|---|
| 10.0 | This command was introduced. |
| 12.2(2)T, 12.0(21)ST, 12.0(22)S | Support for IPv6 was added. |
| 12.2(11)T | The tracert command test characters for IPv6 were updated. New error message was added. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |

Usage Guidelines

The **tracert** command works by taking advantage of the error messages generated by routers when a datagram exceeds its hop limit value.

The **tracert** command starts by sending probe datagrams with a hop limit of one. Including a hop limit of one with a probe datagram causes the neighboring routers to discard the probe datagram and send back an error message. The **tracert** command sends several probes with increasing hop limits and displays the round-trip time for each.

The **tracert** command sends out one probe at a time. Each outgoing packet may result in one or more error messages. A time exceeded error message indicates that an intermediate router has seen and discarded the probe. A destination unreachable error message indicates that the destination node has received and discarded the probe because the hop limit of the packet reached a value of zero. If the timer goes off before a response comes in, the **tracert** command prints an asterisk (*).

The **tracert** command terminates when the destination responds, when the hop limit is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, type Ctrl-^ X—by simultaneously pressing and releasing the Ctrl, Shift, and 6 keys, and then pressing the X key.

To use nondefault parameters and invoke an extended **tracert** test, enter the command without a *protocol* or *destination* argument in privileged EXEC mode. You will be stepped through a dialog to select the desired parameters. Extended **tracert** tests are not supported in user EXEC mode. The user-level **tracert** feature provides a basic trace facility for users that do not have system privileges. The *destination* argument is required in user EXEC mode.

If the system cannot map an address for a host name, it returns an “%No valid source address for destination” message.

Common Tracert Problems

Due to bugs in the IP implementation of various hosts and routers, the IP **tracert** command may behave in an unexpected manner.

Not all destinations will respond correctly to a probe message by sending back an “ICMP port unreachable” message. A long sequence of asterisks, terminating only when the maximum hop limit has been reached, may indicate this problem.

There is a known problem with the way some hosts handle an “ICMP TTL exceeded” message. Some hosts generate an “ICMP” message but they reuse the Time to Live (TTL) of the incoming packet. Because the TTL of the incoming packet is zero, the Internet Control Message Protocol (ICMP) packets do not make it back. When you trace the path to such a host, you may see a set of TTL values with asterisks (*). Eventually the hop limit gets high enough that the “ICMP” message can get back. For example, if the host is six hops away, tracert will time out on responses 6 through 11.



Note

In IPv4, the TTL value can be an amount of time (for example, 250 milliseconds) or a hop count. In IPv6, the equivalent of the TTL value is purely a hop count.

Examples

The following user EXEC example shows IPv4 **tracert** output when a destination host name has been specified:

```
Router> tracert host77-name.domainZZ-name.com
```

Type escape sequence to abort.

Tracing the route to host77-name.domainZZ-name.com (10.0.0.73)

```
 1 host1-name.domain1-name.com (192.168.1.6) 1000 msec 8 msec 4 msec
 2 host33-name.serviceprovider8-name.com (192.168.16.2) 8 msec 8 msec 8 msec
 3 host2-name.college2-name.edu (192.168.110.225) 8 msec 4 msec 4 msec
 4 host44-name.domain2-name.NET (192.168.254.6) 8 msec 8 msec 8 msec
 5 host22-name.serviceprovider99-name.com (192.168.3.8) 12 msec 12 msec 8 msec
 6 host-name5.domain5-name.com (192.168.195.1) 216 msec 120 msec 132 msec
 7 host77-name.domainZZ-name.com (10.0.0.73) 412 msec 628 msec 664 msec
```

Table 123 describes the significant fields shown in the display.

Table 123 *tracert Field Descriptions—IPv4*

| Field | Description |
|-----------------------------|--|
| 1 | Indicates the sequence number of the router in the path to the host. |
| host1-name.domain1-name.com | Host name of this router. |

Table 123 *tracert Field Descriptions—IPv4 (continued)*

| Field | Description |
|-------------------------|--|
| 192.168.1.6 | Internet address of this router. |
| 1000 msec 8 msec 4 msec | Round-trip time for each of the three probes that is sent. |

The following user EXEC example shows IPv6 **tracert** output when a destination host name has been specified:

```
Router> tracert host8-name.domainBB-name.no
```

Type escape sequence to abort.

Tracing the route to host8-name.domainBB-name.no (3FFE:2A00:100:7FF9::2)

```
 1 3FFE:C:00:E:13::2 28 msec 24 msec *
 2 3FFE:2A00:100:7FF8::2 208 msec 204 msec
 3 host32-name.domainHH-name.net (3FFE:2A00:100:7FF8::1) 276 msec * 276 msec
 4 host8-name.domainBB-name.no (3FFE:2A00:100:7FF9::2) 292 msec 292 msec 296 msec
```

**Note**

In the example, host8-name.domainBB-name.no has an IPv6 address, so the protocol for the **tracert** command defaults to IPv6. IPv4 could have been used by specifying **ip** in the **tracert** command; for example, **tracert ip host8-name.domainBB-name.no**.

Table 124 describes the significant fields shown in the display.

Table 124 *tracert Field Descriptions—IPv6*

| Field | Description |
|-----------------------------|--|
| 4 | Indicates the sequence number of the router in the path to the host. |
| host8-name.domainBB-name.no | Host name of the destination node. |
| 3FFE:2A00:100:7FF9::2 | IPv6 address of the destination node. |
| 292 msec 292 msec 296 msec | Round-trip time for each of the three probes that is sent. |

The following privileged EXEC example shows the extended dialog of the **tracert** command when IPv4 is used:

```
Router# tracert
```

Protocol [ip]:

Target IP address: host77-name.domainZZ-name.com

Source address:

Numeric display [n]:

Timeout in seconds [3]:

Probe count [3]:

Minimum Time to Live [1]:

Maximum Time to Live [30]:

Port Number [33434]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Type escape sequence to abort.

Tracing the route to host77-name.domainZZ-name.com (10.0.0.73)

```
 1 host1-name.domain1-name.com (192.168.1.6) 1000 msec 8 msec 4 msec
 2 host33-name.serviceprovider8-name.com (192.168.16.2) 8 msec 8 msec 8 msec
 3 host2-name.college2-name.edu (192.168.110.225) 8 msec 4 msec 4 msec
 4 host44-name.domain2-name.NET (192.168.254.6) 8 msec 8 msec 8 msec
 5 host22-name.serviceprovider99-name.com (192.168.3.8) 12 msec 12 msec 8 msec
```

```

6 host-name5.domain5-name.com (192.168.195.1) 216 msec 120 msec 132 msec
7 host77-name.domainZZ-name.com (10.0.0.73) 412 msec 628 msec 664 msec

```

If an unknown host name is used in the Target IP address field, a Domain Name System (DNS) server is queried to resolve the unknown host name. In the following example, a DNS server (IP address 192.168.7.93) is queried for the unknown host name college9-name.edu:

```
Router# traceroute
```

```
Protocol [ip]:
```

```
Target IP address: college9-name.edu
```

```
Translating "college9-name.edu"...domain server (192.168.7.93) [OK]
```

Table 125 describes the fields that are unique to the extended tracroute sequence, as shown in the display.

Table 125 *traceroute Field Descriptions—IPv4*

| Field | Description |
|---|--|
| Target IP address | You must enter an IPv4 host name or an IPv4 address. There is no default. |
| Source address | One of the interface addresses of the router to use as a source address for the probes. The router will normally choose what it considers to be the best source address to use. |
| Numeric display | The default is to have both a symbolic and numeric display; however, you can suppress the symbolic display. |
| Timeout in seconds | The number of seconds to wait for a response to a probe packet. The default is 3 seconds. |
| Probe count | The number of probes to be sent at each TTL level. The default count is 3. |
| Minimum Time to Live [1] | The TTL value for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops. |
| Maximum Time to Live [30] | The largest TTL value that can be used. The default is 30. The command terminates when the destination is reached or when this value is reached. |
| Port Number | The destination port used by the User Datagram Protocol (UDP) probe messages. The default is 33434. |
| Loose, Strict, Record, Timestamp, Verbose | IP header options. You can specify any combination. The command issues prompts for the required fields. Note that the command will place the requested options in each probe; however, there is no guarantee that all routers (or end nodes) will process the options. |
| Loose | Allows you to specify a list of nodes that must be traversed to the destination. |
| Strict | Allows you to specify a list of nodes that must be the only nodes traversed when going to the destination. |
| Record | Allows you to specify the number of hops to leave room for. |
| Timestamp | Allows you to specify the number of time stamps to leave room for. |
| Verbose | If you select any option, the verbose mode is automatically selected and the command prints the contents of the option field in any incoming packets. You can prevent verbose mode by selecting it again, toggling its current setting. |

The following privileged EXEC example shows the extended dialog of the **tracert** command when IPv6 is used:

```
Router# tracert

Protocol [ip]: ipv6
Target IP address: host8-name.domainBB-name.no
Source IPv6 address:
Numeric display [no]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Priority [0]:
Port Number [33434]:
Type escape sequence to abort.
Tracing the route to host8-name.domainBB-name.no (3FFE:2A00:100:7FF9::2)
 0 3FFE:C:00:E:13::2 28 msec 24 msec *
 1 3FFE:2A00:100:7FF8::2 208 msec 204 msec
 2 host32-name.domainHH-name.net (3FFE:2A00:100:7FF8::1) 276 msec * 276 msec
 3 host8-name.domainBB-name.no (3FFE:2A00:100:7FF9::2) 292 msec 292 msec 296 msec
```

If an unknown host name is used in the Target IP address field, a DNS server is queried to resolve the unknown host name. In the following example, a DNS server (IP address 192.168.7.93) is queried for the unknown host name host8-name.domainBB-name.no:

```
Router# tracert

Protocol [ip]: ipv6
Target IP address: host8-name.domainBB-name.no
Translating "host8-name.domainBB-name.no"...domain server (192.168.7.93) [OK]
```

Table 126 describes the fields that are unique to the extended **tracert** sequence, as shown in the display.

Table 126 *tracert Field Descriptions—IPv6*

| Field | Description |
|---------------------|---|
| Protocol [ip]: | The protocol to use for the probes. The available protocols are appletalk , clns , ip , ipv6 , ipx , oldvines , and vines . The default is ip . |
| Target IP address | You must enter an IPv6 host name or an IPv6 address. There is no default. |
| Source IPv6 address | The IPv6 address of an interface in the router that is used as the source address for the probes. If an address is not entered, the router chooses what it considers to be the best source address to use. Note In Cisco IOS Release 12.2(8)T or later releases, an IPv6 address enclosed in square brackets ([]), such as [FE80::260:3EFF:FE11:6770], is acceptable to the system. Refer to RFC 2732, <i>Format for Literal IPv6 Addresses in URL's</i> , for more information on the use of square brackets with literal IPv6 address in URLs. |
| Numeric display | The default is to have both a symbolic and numeric display; however, you can suppress the symbolic display. |
| Timeout in seconds | The number of seconds to wait for a response to a probe packet. The default is 3 seconds. |

Table 126 *tracert Field Descriptions—IPv6 (continued)*

| Field | Description |
|---------------------------|--|
| Probe count | The number of probes to be sent at each TTL level. The default count is 3. |
| Minimum Time to Live [1] | The HopCount (TTL) value or hop limit for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops. |
| Maximum Time to Live [30] | The largest HopCount (TTL) value or hop limit that can be used. The default is 30. The command terminates when the destination is reached or when this value is reached. |
| Port Number | The destination port used by the UDP probe messages. The default is 33434. |

Table 127 describes the characters that can appear in **tracert** command output when IPv4 is used.

Table 127 *tracert Text Characters—IPv4*

| Character | Description |
|-----------|---|
| nn msec | For each node, the round-trip time (in milliseconds) for the specified number of probes. |
| * | The probe timed out. No response was received within the specified timeout. |
| ? | Unknown error. |
| A | Administratively unreachable. Usually, this output indicates that an access list is blocking traffic. |
| H | Host unreachable. |
| N | Network unreachable (beyond scope). |
| P | Protocol unreachable. |
| Q | Source quench. |
| P | Port unreachable. |

Table 128 describes the characters that can appear in the **tracert** command output when IPv6 is used.

Table 128 *tracert Text Characters—IPv6*

| Character | Description |
|-----------|---|
| ! | Indicates receipt of a reply. |
| * | The probe timed out. No response was received within the specified timeout. |
| ? | Unknown error. |
| @ | Unreachable for unknown reason. |
| A | Administratively unreachable. Usually, this output indicates that an access list is blocking traffic. |
| H | Host unreachable. |
| N | Network unreachable (beyond scope). |

Table 128 *tracert Text Characters—IPv6 (continued)*

| Character | Description |
|-----------|-------------------|
| P | Port unreachable. |
| U | No route to host. |

tunnel mode ipv6ip

To configure a static IPv6 tunnel interface, use the **tunnel mode ipv6ip** command in interface configuration mode. To remove an IPv6 tunnel interface, use the **no** form of this command.

tunnel mode ipv6ip [**6to4** | **auto-tunnel** | **isatap**]

no tunnel mode ipv6ip

| | | |
|---------------------------|--------------------|--|
| Syntax Description | 6to4 | (Optional) Specifies IPv6 automatic tunneling mode using a 6to4 address. |
| | auto-tunnel | (Optional) Specifies IPv6 automatic tunneling mode using an IPv4-compatible IPv6 address. |
| | isatap | (Optional) Specifies IPv6 automatic tunneling mode as Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) to connect IPv6 nodes (hosts and routers) within IPv4 networks. |

Defaults IPv6 tunnel interfaces are not configured.

Command Modes Interface configuration

| | | |
|------------------------|----------------|---|
| Command History | Release | Modification |
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | The ISATAP keyword was added to support the addition of ISATAP tunnel implementation. |

Usage Guidelines IPv6 tunneling consists of encapsulating IPv6 packets within IPv4 packets for transmission across an IPv4 routing infrastructure.

Manually Configured Tunnels

Using the **tunnel mode ipv6ip** command without keywords specifies an IPv6 configured tunnel where a manually configured IPv6 address is configured on a tunnel interface and manually configured IPv4 addresses are configured as the tunnel source and the tunnel destination. The host or router at each end of an IPv6 configured tunnel must support both the IPv4 and IPv6 protocol stacks.

Automatic Determination of Tunnel Source and Destination

Using the **tunnel mode ipv6ip** command with the **auto-tunnel** keyword specifies an IPv6 automatic tunnel where the tunnel destination is automatically determined by the IPv4 address in the low-order 32 bits of IPv4-compatible IPv6 addresses. An IPv4-compatible IPv6 address is a 128-bit IPv6 address that contains the IPv6 prefix 0:0:0:0:0:0 in the high-order 96 bits of the address and an IPv4 address in the low-order 32 bits of the address. The host or router at each end of an automatic tunnel must support both the IPv4 and IPv6 protocol stacks.

6to4 Tunnels

Using the **tunnel mode ipv6ip** command with the **6to4** keyword specifies automatic 6to4 tunneling where the tunnel endpoint is determined by the globally unique IPv4 address embedded in a 6to4 address. A 6to4 address is a combination of the prefix 2002::/16 and a globally unique 32-bit IPv4 address. (IPv4-compatible addresses are not used in 6to4 tunneling.) The unique IPv4 address is used as the network-layer address in the 6to4 address prefix. The border router at each end of a 6to4 tunnel must support both the IPv4 and IPv6 protocol stacks. The 6to4 tunnel must be configured with the **tunnel source** command to use an interface with an IPv4 address as the source of the tunnel. Additionally, the 6to4 address prefix must be routed over the tunnel using the **ipv6 route** command.

ISATAP Tunnels

ISATAP tunnels enable transport of IPv6 packets within network boundaries. ISATAP tunnels allow individual IPv4/IPv6 dual-stack hosts within a site to connect to an IPv6 network using the IPv4 infrastructure.

Unlike IPv4-compatible addresses, ISATAP IPv6 addresses can use any initial unicast /64 prefix. The final 64 bits are an interface identifier. Of these, the leading 32 bits are the fixed pattern 0000:5EFE; the last 32 bits carry the tunnel endpoint IPv4 address.

Examples

Manually Configured IPv6 Tunnel Example

The following example configures a manual IPv6 tunnel. In the example, tunnel interface 0 is manually configured with a global IPv6 address. The tunnel source and destination are also manually configured.

```
Router(config)# interface tunnel 0
Router(config-if)# ipv6 address 3ffe:b00:c18:1::3/127
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel destination 192.168.30.1
Router(config-if)# tunnel mode ipv6ip
```

IPv4 Compatible IPv6 Address Tunnel Example

The following example configures an automatic IPv6 tunnel that uses Ethernet interface 0 as the tunnel source. The tunnel destination is automatically determined by the IPv4 address in the low-order 32 bits of an IPv4-compatible IPv6 address.

```
Router(config)# interface tunnel 0
Router(config-if)# no ip address
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel mode ipv6ip auto-tunnel
```

6to4 Tunnel Example

The following example configures a 6to4 tunnel. 6to4 tunnels allows for autoconfiguration where a site-specific 48-bit prefix is dynamically constructed by prepending the prefix 2002 to an IPv4 address assigned to the site. In the example, Ethernet interface 0 is configured with an IPv4 address, and with a 64-bit prefix (/64) which is part of the previously constructed 48-bit prefix (/48). Tunnel interface 0 is configured without an IPv4 or IPv6 address because the IPv4 or IPv6 addresses on Ethernet interface 0 is used to construct a tunnel source address. A tunnel destination address is not specified because the destination address is automatically constructed. An IPv6 static route for network 2002::/16 to tunnel interface 0 is configured (traffic destined for the prefix is routed over tunnel interface 0).

```
Router(config)# interface ethernet 0
Router(config-if)# ip address 192.168.99.1 255.255.255.0
Router(config-if)# ipv6 address 2002:c0a8:6301:1::/64 eui-64
Router(config-if)# exit
Router(config)# interface tunnel 0
```



```

Router(config-if)# no ip address
Router(config-if)# ipv6 unnumbered ethernet 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel mode ipv6ip 6to4
Router(config-if)# exit
Router(config)# ipv6 route 2002::/16 tunnel 0

```

Tunnel Interface Configured with the ipv6 unnumbered Command Example

When a tunnel interface is configured using the **ipv6 unnumbered** command with the **tunnel source** and **tunnel mode ipv6ip** commands, the tunnel uses the first IPv6 address configured on the source interface as its IPv6 address. For 6to4 tunnels, the first IPv6 address configured on the source interface must be a 6to4 address. In the following example, the first IPv6 address configured for Ethernet interface 0 (6to4 address 2002:c0a8:6301:1::/64) is used as the IPv6 address of tunnel 0:

```

Router(config)# interface tunnel 0
Router(config-if)# ipv6 unnumbered ethernet 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel mode ipv6ip 6to4
Router(config-if)# exit
Router(config)# interface ethernet 0
Router(config-if)# ipv6 address 2002:c0a8:6301:1::/64 eui-64
Router(config-if)# ipv6 address 3ffe:1234:5678::1/64

```

ISATAP Tunnel Example

The following command shows an ISATAP tunnel configured on interface Ethernet 0. Router advertisements are enabled to allow client autoconfiguration.

```

Router(config)# interface Ethernet 0
Router(config-if)# ip address 1.1.1.1 255.255.255.0
Router(config)# interface Tunnel 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel mode ipv6ip isatap
Router(config-if)# ipv6 address 2001:0DB8::/64 eiu-64
Router(config-if)# no ipv6 nd suppress-ra

```

Related Commands

| Command | Description |
|----------------------------|--|
| ip address | Specifies the IP address of an IPv4 interface. |
| ipv6 address eui-64 | Configures an IPv6 address for an interface and enables IPv6 processing on the interface using an EUI-64 interface ID in the low order 64 bits of the address. |
| ipv6 unnumbered | Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface. |
| show ipv6 interface | Displays the usability status of interfaces configured for IPv6. |
| tunnel destination | Sets the destination address for a tunnel interface. |
| tunnel source | Sets the source address for a tunnel interface. |