



IPv6 Addressing and Basic Connectivity Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 1000)

Americas Headquarters

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

IPv6 Addressing and Basic Connectivity 1

Finding Feature Information 1

Restrictions for Implementing IPv6 Addressing and Basic Connectivity 1

Information About IPv6 Addressing and Basic Connectivity 2

IPv6 for Cisco Software 2

Large IPv6 Address Space for Unique Addresses 2

IPv6 Address Formats 3

IPv6 Address Output Display 4

Simplified IPv6 Packet Header 4

DNS for IPv6 8

Cisco Discovery Protocol IPv6 Address Support 8

IPv6 Prefix Aggregation 9

IPv6 Site Multihoming 9

IPv6 Data Links 9

Dual IPv4 and IPv6 Protocol Stacks 10

How to Configure IPv6 Addressing and Basic Connectivity 11

Configuring IPv6 Addressing and Enabling IPv6 Routing 11

Mapping Hostnames to IPv6 Addresses 14

Hostname-to-Address Mappings 14

Displaying IPv6 Redirect Messages 16

Configuration Examples for IPv6 Addressing and Basic Connectivity 17

Example: IPv6 Addressing and IPv6 Routing Configuration 18

Example: Dual-Protocol Stacks Configuration 18

Example: Hostname-to-Address Mappings Configuration 18

Additional References 18

Feature Information for IPv6 Addressing and Basic Connectivity 20

IPv6 Anycast Address 23

Finding Feature Information 23

Information About IPv6 Anycast Address 23

IPv6 Address Type: Anycast	23
How to Configure IPv6 Anycast Address	24
Configuring IPv6 Anycast Addressing	24
Configuration Examples for IPv6 Anycast Address	25
Example: Configuring IPv6 Anycast Addressing	25
Additional References	26
Feature Information for IPv6 Anycast Address	27
IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support	29
Finding Feature Information	29
Prerequisites for IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support	29
Information About IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support	30
Cisco Express Forwarding and Distributed Cisco Express Forwarding Switching for IPv6	30
How to Configure IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support	31
Configuring Cisco Express Forwarding Switching on Distributed and Nondistributed Architecture Platforms	31
Configuration Examples for IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support	32
Example: Cisco Express Forwarding and Distributed Cisco Express Forwarding Configuration	33
Additional References	33
Feature Information for IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support	34
Unicast Reverse Path Forwarding for IPv6	37
Finding Feature Information	37
Prerequisites for Unicast Reverse Path Forwarding for IPv6	37
Information About Unicast Reverse Path Forwarding for IPv6	38
Unicast Reverse Path Forwarding	38
How to Configure Unicast Reverse Path Forwarding for IPv6	38
Configuring Unicast RPF	39
Configuration Examples for Unicast Reverse Path Forwarding for IPv6	40
Example: Configuring Unicast Reverse Path Forwarding for IPv6	40
Additional References	40

Feature Information for Unicast Reverse Path Forwarding for IPv6	41
IPv6 Services: AAAA DNS Lookups over an IPv4 Transport	43
Finding Feature Information	43
Information About IPv6 Services: AAAA DNS Lookups over an IPv4 Transport	43
DNS for IPv6	43
Additional References	44
Feature Information for IPv6 Services: AAAA DNS Lookups over an IPv4 Transport	45
IPv6 MTU Path Discovery	47
Finding Feature Information	47
Information About IPv6 MTU Path Discovery	47
IPv6 MTU Path Discovery	47
ICMP for IPv6	48
How to Configure IPv6 MTU Path Discovery	49
Enabling Flow-Label Marking in Packets that Originate from the Device	49
Configuration Examples for IPv6 MTU Path Discovery	50
Example: Displaying IPv6 Interface Statistics	50
Additional References	50
Feature Information for IPv6 MTU Path Discovery	51
ICMP for IPv6	53
Finding Feature Information	53
Information About ICMP for IPv6	53
ICMP for IPv6	53
IPv6 Neighbor Solicitation Message	54
IPv6 Router Advertisement Message	56
Default Router Preferences for Traffic Engineering	57
Additional References	57
Feature Information for ICMP for IPv6	58
IPv6 ICMP Rate Limiting	61
Finding Feature Information	61
Information About IPv6 ICMP Rate Limiting	61
ICMP for IPv6	61
IPv6 ICMP Rate Limiting	62
How to Configure IPv6 ICMP Rate Limiting	62
Customizing IPv6 ICMP Rate Limiting	63
Configuration Examples for IPv6 ICMP Rate Limiting	63
Example: IPv6 ICMP Rate Limiting Configuration	63

Example: Displaying Information About ICMP Rate-Limited Counters	63
Additional References	64
Feature Information for IPv6 ICMP Rate Limiting	65
ICMP for IPv6 Redirect	67
Finding Feature Information	67
Information About ICMP for IPv6 Redirect	67
ICMP for IPv6	67
IPv6 Neighbor Redirect Message	68
How to Display IPv6 Redirect Messages	69
Displaying IPv6 Redirect Messages	69
Configuration Examples for ICMP for IPv6 Redirect	71
Example: Displaying IPv6 Interface Statistics	71
Additional References	71
Feature Information for ICMP for IPv6 Redirect	72
IPv6 Neighbor Discovery	75
Finding Feature Information	75
Information About IPv6 Neighbor Discovery	75
IPv6 Neighbor Discovery	75
IPv6 Neighbor Solicitation Message	76
IPv6 Router Advertisement Message	77
Default Router Preferences for Traffic Engineering	79
IPv6 Neighbor Redirect Message	79
How to Configure IPv6 Neighbor Discovery	80
Tuning the Parameters for IPv6 Neighbor Discovery	80
Customizing IPv6 ICMP Rate Limiting	81
Displaying IPv6 Redirect Messages	82
Configuration Examples for IPv6 Neighbor Discovery	84
Example: Customizing the Parameters for IPv6 Neighbor Discovery	84
Example: IPv6 ICMP Rate Limiting Configuration	84
Example: Displaying Information About ICMP Rate-Limited Counters	84
Example: Displaying IPv6 Interface Statistics	85
Additional References	85
Feature Information for IPv6 Neighbor Discovery	86
IPv6 Neighbor Discovery Cache	89
Finding Feature Information	89

Information About IPv6 Static Cache Entry for Neighbor Discovery	89
IPv6 Neighbor Discovery	89
Per-Interface Neighbor Discovery Cache Limit	90
How to Configure IPv6 Neighbor Discovery Cache	90
Configuring a Neighbor Discovery Cache Limit on a Specified Interface	90
Configuring a Neighbor Discovery Cache Limit on All Device Interfaces	91
Configuration Examples for IPv6 Neighbor Discovery Cache	92
Example: Configuring a Neighbor Discovery Cache Limit	92
Additional References	92
Feature Information for IPv6 Neighbor Discovery Cache	93
IPv6 Stateless Autoconfiguration	95
Finding Feature Information	95
Information About IPv6 Stateless Autoconfiguration	95
IPv6 Stateless Autoconfiguration	95
Simplified Network Renumbering for IPv6 Hosts	96
How to Configure IPv6 Stateless Autoconfiguration	96
Enabling IPv6 Stateless Autoconfiguration	96
Configuration Examples for IPv6 Stateless Autoconfiguration	97
Example: Displaying IPv6 Interface Statistics	97
Additional References	98
Feature Information for IPv6 Stateless Autoconfiguration	99



IPv6 Addressing and Basic Connectivity

Internet Protocol version 6 (IPv6) expands the number of network address bits from 32 bits (in IPv4) to 128 bits, which provides more than enough globally unique IP addresses for every networked device on the planet. The unlimited address space provided by IPv6 allows Cisco to deliver more and newer applications and services with reliability, improved user experience, and increased security.

Implementing basic IPv6 connectivity in the Cisco software consists of assigning IPv6 addresses to individual device interfaces. IPv6 traffic forwarding can be enabled globally, and Cisco Express Forwarding switching for IPv6 can also be enabled. The user can enhance basic connectivity functionality by configuring support for AAAA record types in the Domain Name System (DNS) name-to-address and address-to-name lookup processes, and by managing IPv6 neighbor discovery.

- [Finding Feature Information, page 1](#)
- [Restrictions for Implementing IPv6 Addressing and Basic Connectivity, page 1](#)
- [Information About IPv6 Addressing and Basic Connectivity, page 2](#)
- [How to Configure IPv6 Addressing and Basic Connectivity, page 11](#)
- [Configuration Examples for IPv6 Addressing and Basic Connectivity, page 17](#)
- [Additional References, page 18](#)
- [Feature Information for IPv6 Addressing and Basic Connectivity, page 20](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Implementing IPv6 Addressing and Basic Connectivity

- IPv6 packets are transparent to Layer 2 LAN switches because the switches do not examine Layer 3 packet information before forwarding IPv6 frames. Therefore, IPv6 hosts can be directly attached to Layer 2 LAN switches.
- Multiple IPv6 global addresses within the same prefix can be configured on an interface; however, multiple IPv6 link-local addresses on an interface are not supported.

Information About IPv6 Addressing and Basic Connectivity

- [IPv6 for Cisco Software, page 2](#)
- [Large IPv6 Address Space for Unique Addresses, page 2](#)
- [IPv6 Address Formats, page 3](#)
- [IPv6 Address Output Display, page 4](#)
- [Simplified IPv6 Packet Header, page 4](#)
- [DNS for IPv6, page 8](#)
- [Cisco Discovery Protocol IPv6 Address Support, page 8](#)
- [IPv6 Prefix Aggregation, page 9](#)
- [IPv6 Site Multihoming, page 9](#)
- [IPv6 Data Links, page 9](#)
- [Dual IPv4 and IPv6 Protocol Stacks, page 10](#)

IPv6 for Cisco Software

IPv6, formerly named IPng (next generation), is the latest version of the Internet Protocol (IP). IP is a packet-based protocol used to exchange data, voice, and video traffic over digital networks. IPv6 was proposed when it became clear that the 32-bit addressing scheme of IP version 4 (IPv4) was inadequate to meet the demands of Internet growth. After extensive discussion it was decided to base IPng on IP but add a much larger address space and improvements such as a simplified main header and extension headers. IPv6 is described initially in RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*, issued by the Internet Engineering Task Force (IETF). Further RFCs describe the architecture and services supported by IPv6.

The architecture of IPv6 has been designed to allow existing IPv4 users to transition easily to IPv6 while providing services such as end-to-end security, quality of service (QoS), and globally unique addresses. The larger IPv6 address space allows networks to scale and provide global reachability. The simplified IPv6 packet header format handles packets more efficiently. IPv6 prefix aggregation, simplified network renumbering, and IPv6 site multihoming capabilities provide an IPv6 addressing hierarchy that allows for more efficient routing. IPv6 supports widely deployed routing protocols such as Routing Information Protocol (RIP), Integrated Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF) for IPv6, and multiprotocol Border Gateway Protocol (BGP). Other available features include stateless autoconfiguration and an increased number of multicast addresses.

Large IPv6 Address Space for Unique Addresses

The primary motivation for IPv6 is the need to meet the demand for globally unique IP addresses. IPv6 quadruples the number of network address bits from 32 bits (in IPv4) to 128 bits, which provides more than enough globally unique IP addresses for every networked device on the planet. By being globally unique, IPv6 addresses inherently enable global reachability and end-to-end security for networked devices, functionality that is crucial to the applications and services that are driving the demand for the addresses. Additionally, the flexibility of the IPv6 address space reduces the need for private addresses; therefore, IPv6 enables new application protocols that do not require special processing by border devices at the edge of networks.

IPv6 Address Formats

IPv6 addresses are represented as a series of 16-bit hexadecimal fields separated by colons (:) in the format: x:x:x:x:x:x:x. Following are two examples of IPv6 addresses:

2001:DB8:7654:3210:FEDC:BA98:7654:3210

2001:DB8:0:0:8:800:200C:417A

IPv6 addresses commonly contain successive hexadecimal fields of zeros. Two colons (::) may be used to compress successive hexadecimal fields of zeros at the beginning, middle, or end of an IPv6 address (the colons represent successive hexadecimal fields of zeros). The table below lists compressed IPv6 address formats.

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.



Note

Two colons (::) can be used only once in an IPv6 address to represent the longest successive hexadecimal fields of zeros. The hexadecimal letters in IPv6 addresses are not case-sensitive.

Table 1 **Compressed IPv6 Address Formats**

IPv6 Address Type	Preferred Format	Compressed Format
Unicast	2001:0:0:0:DB8:800:200C:417A	2001::DB8:800:200C:417A
Multicast	FF01:0:0:0:0:0:0:101	FF01::101
Loopback	0:0:0:0:0:0:0:1	::1
Unspecified	0:0:0:0:0:0:0:0	::

The loopback address listed in the table above may be used by a node to send an IPv6 packet to itself. The loopback address in IPv6 functions the same as the loopback address in IPv4 (127.0.0.1).



Note

The IPv6 loopback address cannot be assigned to a physical interface. A packet that has the IPv6 loopback address as its source or destination address must remain within the node that created the packet. IPv6 devices do not forward packets that have the IPv6 loopback address as their source or destination address.

The unspecified address listed in the table above indicates the absence of an IPv6 address. For example, a newly initialized node on an IPv6 network may use the unspecified address as the source address in its packets until it receives its IPv6 address.



Note

The IPv6 unspecified address cannot be assigned to an interface. The unspecified IPv6 addresses must not be used as destination addresses in IPv6 packets or the IPv6 routing header.

An IPv6 address prefix, in the format *ipv6-prefix/prefix-length*, can be used to represent bit-wise contiguous blocks of the entire address space. The *ipv6-prefix* must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. The prefix length is

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). For example, 2001:DB8:8086:6502::/32 is a valid IPv6 prefix.

IPv6 Address Output Display

When IPv6 or IPv4 command output displays an IPv6 address, a long IPv6 address can overflow into neighboring fields, causing the output to be difficult to read. The output fields were designed to work with the longest possible IPv4 address, which has 15 characters; IPv6 addresses can be up to 39 characters long. The following scheme has been adopted in IPv4 and IPv6 commands to allow the appropriate length of IPv6 address to be displayed and move the following fields to the next line, if necessary. The fields that are moved are kept in alignment with the header row.

The following example displays eight connections. The first six connections feature IPv6 addresses; the last two connections feature IPv4 addresses.

```
Device# where
Conn Host                Address                Byte  Idle Conn Name
  1 test5                2001:DB8:3333:4::5    6     24 test5
  2 test4                2001:DB8:3333:44::5
                                6     24 test4
  3 2001:DB8:3333:4::5 2001:DB8:3333:4::5    6     24 2001:DB8:3333:4::5
  4 2001:DB8:3333:44::5
                                2001:DB8:3333:44::5
                                6     23 2001:DB8:3333:44::5
  5 2001:DB8:3000:4000:5000:6000:7000:8001
                                2001:DB8:3000:4000:5000:6000:7000:8001
                                6     20 2001:DB8:3000:4000:5000:6000:
  6 2001:DB8:1::1        2001:DB8:1::1         0      1 2001:DB8:1::1
  7 10.1.9.1             10.1.9.1              0      0 10.1.9.1
  8 10.222.111.222       10.222.111.222        0      0 10.222.111.222
```

Connection 1 contains an IPv6 address that uses the maximum address length in the address field. Connection 2 shows the IPv6 address overflowing the address field and the following fields moved to the next line, but in alignment with the appropriate headers. Connection 3 contains an IPv6 address that fills the maximum length of the hostname and address fields without wrapping any lines. Connection 4 shows the effect of both the hostname and address fields containing a long IPv6 address. The output is shown over three lines keeping the correct heading alignment. Connection 5 displays a similar effect as connection 4 with a very long IPv6 address in the hostname and address fields. Note that the connection name field is actually truncated. Connection 6 displays a very short IPv6 address that does not require any change in the display. Connections 7 and 8 display short and long IPv4 addresses.



Note

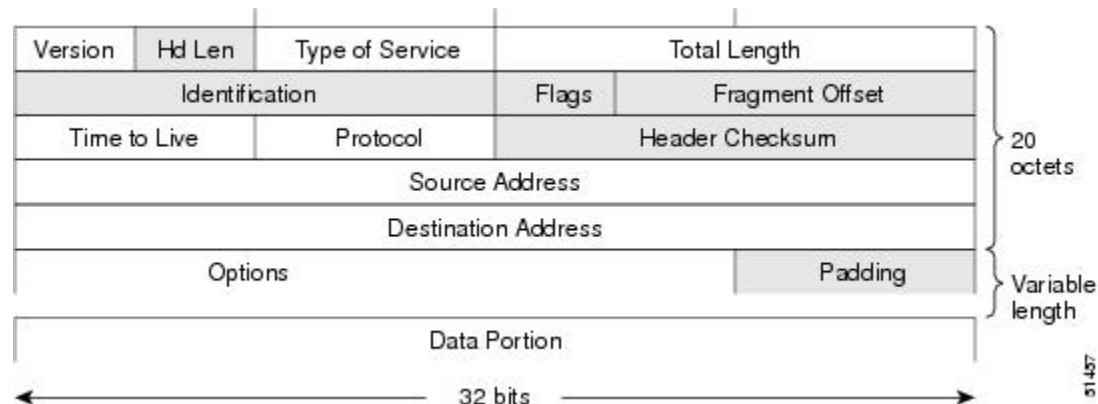
The IPv6 address output display applies to all commands that display IPv6 addresses.

Simplified IPv6 Packet Header

The basic IPv4 packet header has 12 fields with a total size of 20 octets (160 bits) (see the figure below). The 12 fields may be followed by an Options field, which is followed by a data portion that is usually the transport-layer packet. The variable length of the Options field adds to the total size of the IPv4 packet

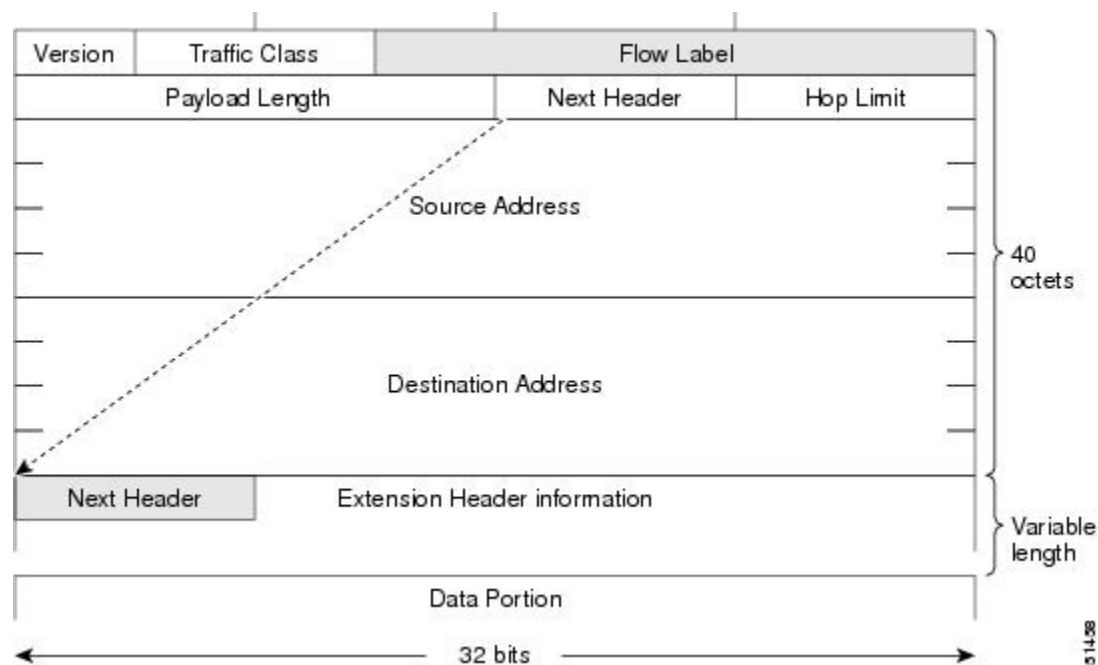
header. The shaded fields of the IPv4 packet header shown in the figure below are not included in the IPv6 packet header.

Figure 1 IPv4 Packet Header Format



The basic IPv6 packet header has 8 fields with a total size of 40 octets (320 bits) (see the figure below). Fields were removed from the IPv6 header because, in IPv6, fragmentation is not handled by devices and checksums at the network layer are not used. Instead, fragmentation in IPv6 is handled by the source of a packet and checksums at the data link layer and transport layer are used. (In IPv4, the UDP transport layer uses an optional checksum. In IPv6, use of the UDP checksum is required to check the integrity of the inner packet.) Additionally, the basic IPv6 packet header and Options field are aligned to 64 bits, which can facilitate the processing of IPv6 packets.

Figure 2 IPv6 Packet Header Format



The table below lists the fields in the basic IPv6 packet header.

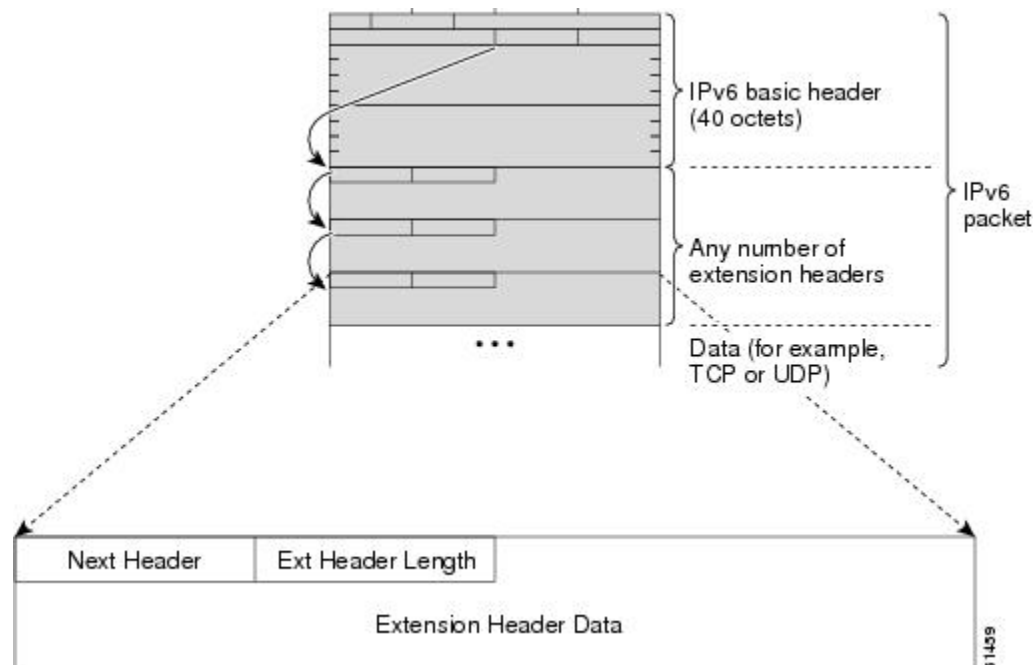
Table 2 **Basic IPv6 Packet Header Fields**

Field	Description
Version	Similar to the Version field in the IPv4 packet header, except that the field lists number 6 for IPv6 instead of number 4 for IPv4.
Traffic Class	Similar to the Type of Service field in the IPv4 packet header. The Traffic Class field tags packets with a traffic class that is used in differentiated services.
Flow Label	A new field in the IPv6 packet header. The Flow Label field tags packets with a specific flow that differentiates the packets at the network layer.
Payload Length	Similar to the Total Length field in the IPv4 packet header. The Payload Length field indicates the total length of the data portion of the packet.
Next Header	Similar to the Protocol field in the IPv4 packet header. The value of the Next Header field determines the type of information following the basic IPv6 header. The type of information following the basic IPv6 header can be a transport-layer packet, for example, a TCP or UDP packet, or an Extension Header, as shown in the figure immediately above.
Hop Limit	Similar to the Time to Live field in the IPv4 packet header. The value of the Hop Limit field specifies the maximum number of devices that an IPv6 packet can pass through before the packet is considered invalid. Each device decrements the value by one. Because no checksum is in the IPv6 header, the device can decrement the value without needing to recalculate the checksum, which saves processing resources.
Source Address	Similar to the Source Address field in the IPv4 packet header, except that the field contains a 128-bit source address for IPv6 instead of a 32-bit source address for IPv4.
Destination Address	Similar to the Destination Address field in the IPv4 packet header, except that the field contains a 128-bit destination address for IPv6 instead of a 32-bit destination address for IPv4.

Following the eight fields of the basic IPv6 packet header are optional extension headers and the data portion of the packet. If present, each extension header is aligned to 64 bits. There is no fixed number of extension headers in an IPv6 packet. The extension headers form a chain of headers. Each extension header is identified by the Next Header field of the previous header. Typically, the final extension header has a

Next Header field of a transport-layer protocol, such as TCP or UDP. The figure below shows the IPv6 extension header format.

Figure 3 IPv6 Extension Header Format



The table below lists the extension header types and their Next Header field values.

Table 3 IPv6 Extension Header Types

Header Type	Next Header Value	Description
Hop-by-hop options header	0	This header is processed by all hops in the path of a packet. When present, the hop-by-hop options header always follows immediately after the basic IPv6 packet header.
Destination options header	60	The destination options header can follow any hop-by-hop options header, in which case the destination options header is processed at the final destination and also at each visited address specified by a routing header. Alternatively, the destination options header can follow any Encapsulating Security Payload (ESP) header, in which case the destination options header is processed only at the final destination.
Routing header	43	The routing header is used for source routing.

Header Type	Next Header Value	Description
Fragment header	44	The fragment header is used when a source must fragment a packet that is larger than the maximum transmission unit (MTU) for the path between itself and a destination. The Fragment header is used in each fragmented packet.
Authentication header and ESP header	51 50	The Authentication header and the ESP header are used within IP Security Protocol (IPsec) to provide authentication, integrity, and confidentiality of a packet. These headers are identical for both IPv4 and IPv6.
Upper-layer headers	6 (TCP) 17 (UDP)	The upper-layer (transport) headers are the typical headers used inside a packet to transport the data. The two main transport protocols are TCP and UDP.
Mobility headers	135	Extension headers used by mobile nodes, correspondent nodes, and home agents in all messaging related to the creation and management of bindings.

DNS for IPv6

IPv6 supports DNS record types that are supported in the DNS name-to-address and address-to-name lookup processes. The DNS record types support IPv6 addresses. IPv6 also supports the reverse mapping of IPv6 addresses to DNS names.

The table below lists the IPv6 DNS record types.

Table 4 **IPv6 DNS Record Types**

Record Type	Description	Format
AAAA	Maps a hostname to an IPv6 address. (Equivalent to an A record in IPv4.)	www.abc.test AAAA 3FFE:YYYY:C18:1::2
PTR	Maps an IPv6 address to a hostname. (Equivalent to a PTR record in IPv4.) Note Cisco software supports resolution of PTR records for the IP6.INT domain.	2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1. c.0.y.y.y.e.f.f.3.ip6.int PTR www.abc.test

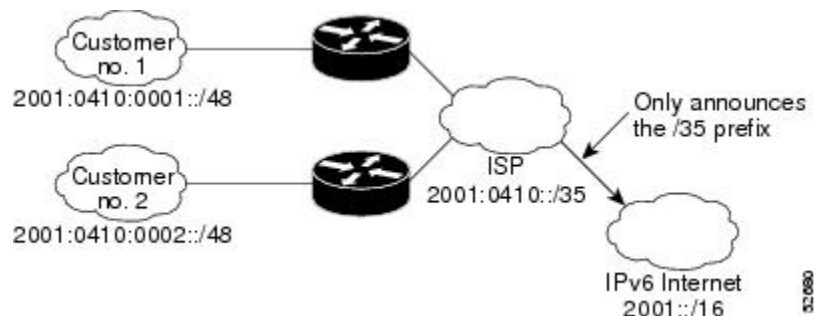
Cisco Discovery Protocol IPv6 Address Support

The Cisco Discovery Protocol IPv6 address support for neighbor information feature adds the ability to transfer IPv6 addressing information between two Cisco devices. Cisco Discovery Protocol support for IPv6 addresses provides IPv6 information to network management products and troubleshooting tools.

IPv6 Prefix Aggregation

The aggregatable nature of the IPv6 address space enables an IPv6 addressing hierarchy. For example, an enterprise can subdivide a single IPv6 prefix from a service provider into multiple, longer prefixes for use within its internal network. Conversely, a service provider can aggregate all of the prefixes of its customers into a single, shorter prefix that the service provider can then advertise over the IPv6 internet (see the figure below).

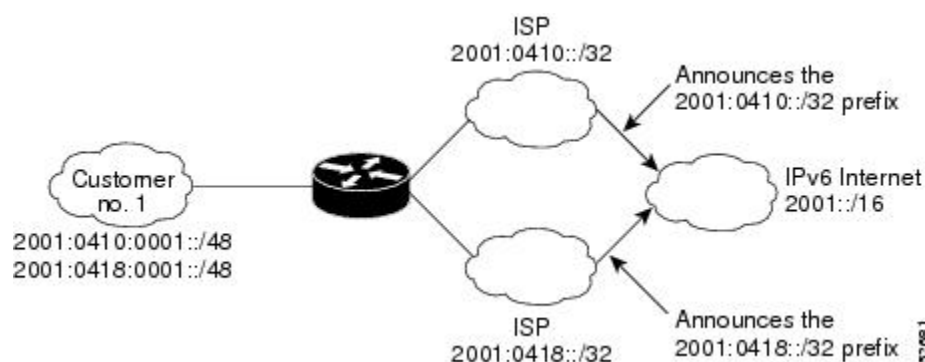
Figure 4 IPv6 Prefix Aggregation



IPv6 Site Multihoming

Multiple IPv6 prefixes can be assigned to networks and hosts. Having multiple prefixes assigned to a network allows that network to connect easily to multiple ISPs without breaking the global routing table (see the figure below).

Figure 5 IPv6 Site Multihoming



IPv6 Data Links

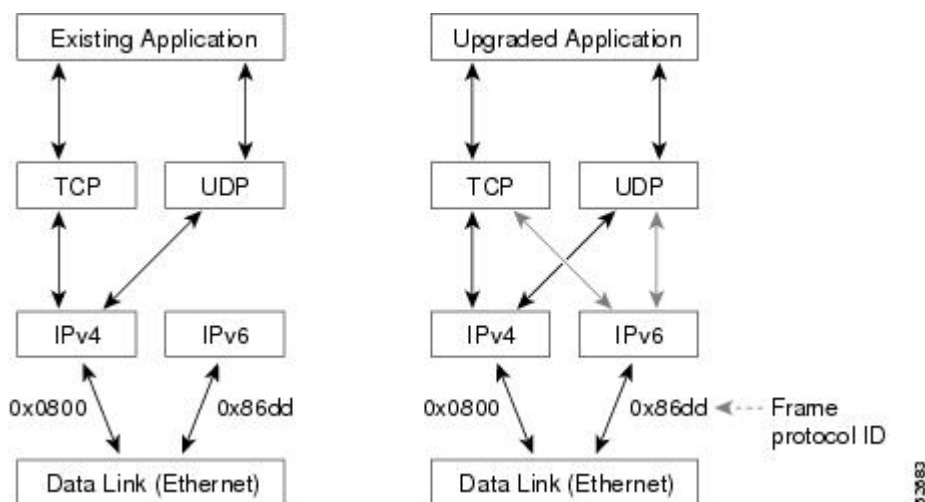
In IPv6 networks, a data link is a network sharing a particular link-local prefix. Data links are networks arbitrarily segmented by a network administrator in order to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks. The function of a subnetwork in IPv6 is similar to a subnetwork in IPv4. A subnetwork prefix is associated with one data link; multiple subnetwork prefixes may be assigned to the same data link.

The following data links are supported for IPv6: FDDI, Frame Relay PVC, Cisco High-Level Data Link Control (HDLC), PPP over Packet over SONET, ISDN, and serial interfaces.

Dual IPv4 and IPv6 Protocol Stacks

The dual IPv4 and IPv6 protocol stack technique can be used to transition to IPv6. It enables gradual, one-by-one upgrades to applications running on nodes. Applications running on nodes are upgraded to make use of the IPv6 protocol stack. Applications that are not upgraded (for example, they support only the IPv4 protocol stack) can coexist with upgraded applications on a node. New and upgraded applications make use of both the IPv4 and IPv6 protocol stacks (see the figure below).

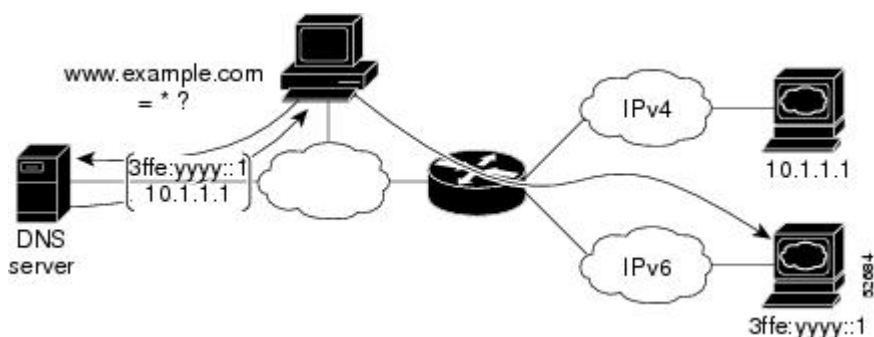
Figure 6 Dual IPv4 and IPv6 Protocol Stack Technique



One application program interface (API) supports both IPv4 and IPv6 addresses and DNS requests. An application can be upgraded to the new API and still use only the IPv4 protocol stack. The Cisco software supports the dual IPv4 and IPv6 protocol stack technique. When an interface is configured with both an IPv4 and an IPv6 address, the interface will forward both IPv4 and IPv6 traffic.

In the figure below, an application that supports dual IPv4 and IPv6 protocol stacks requests all available addresses for the destination hostname `www.example.com` from a DNS server. The DNS server replies with all available addresses (both IPv4 and IPv6 addresses) for `www.example.com`. The application chooses an address (in most cases, IPv6 addresses are the default choice), and connects the source node to the destination using the IPv6 protocol stack.

Figure 7 Dual IPv4 and IPv6 Protocol Stack Applications



How to Configure IPv6 Addressing and Basic Connectivity

- [Configuring IPv6 Addressing and Enabling IPv6 Routing, page 11](#)
- [Mapping Hostnames to IPv6 Addresses, page 14](#)
- [Displaying IPv6 Redirect Messages, page 16](#)

Configuring IPv6 Addressing and Enabling IPv6 Routing

Perform this task to assign IPv6 addresses to individual device interfaces and enable IPv6 traffic forwarding globally on the device. By default, IPv6 addresses are not configured and IPv6 routing is disabled.

**Note**

Multiple IPv6 link-local addresses on an interface are not supported.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Do one of the following:
 - **ipv6 address** *ipv6-prefix /prefix-length eui-64*
 -
 - **ipv6 address** *ipv6-address / prefix-length link-local*
 -
 -
 - **ipv6 enable**
5. **exit**
6. **ipv6 unicast-routing**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.

Command or Action	Purpose
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3 interface <i>type number</i> Example: Device(config)# interface gigabitethernet 0/0/0	Specifies an interface type and number, and places the device in interface configuration mode.

Command or Action	Purpose
<p>Step 4 Do one of the following:</p> <ul style="list-style-type: none"> • ipv6 address <i>ipv6-prefix /prefix-length</i> eui-64 • • ipv6 address <i>ipv6-address / prefix-length</i> link-local • • • ipv6 enable <p>Example:</p> <pre>Device(config-if)# ipv6 address 2001:DB8:0:1::/64 eui-64</pre> <p>Example:</p> <p>Example:</p> <pre>Device(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local</pre> <p>Example:</p> <p>Example:</p> <pre>Device(config-if)# ipv6 enable</pre>	<p>Specifies an IPv6 network assigned to the interface and enables IPv6 processing on the interface.</p> <p>or</p> <p>Specifies an IPv6 address assigned to the interface and enables IPv6 processing on the interface.</p> <p>or</p> <p>Automatically configures an IPv6 link-local address on the interface while also enabling the interface for IPv6 processing. The link-local address can be used only to communicate with nodes on the same link.</p> <ul style="list-style-type: none"> • Specifying the ipv6 address eui-64 command configures global IPv6 addresses with an interface identifier (ID) in the low-order 64 bits of the IPv6 address. Only the 64-bit network prefix for the address needs to be specified; the last 64 bits are automatically computed from the interface ID. • Specifying the ipv6 address link-local command configures a link-local address on the interface that is used instead of the link-local address that is automatically configured when IPv6 is enabled on the interface.
<p>Step 5 exit</p> <p>Example:</p> <pre>Device(config-if)# exit</pre>	<p>Exits interface configuration mode, and returns the device to global configuration mode.</p>

Command or Action	Purpose
Step 6 ipv6 unicast-routing Example: Device(config)# ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams.

Mapping Hostnames to IPv6 Addresses

- [Hostname-to-Address Mappings, page 14](#)

Hostname-to-Address Mappings

A name server is used to track information associated with domain names. A name server can maintain a database of hostname-to-address mappings. Each name can map to one or more IPv4 addresses, IPv6 addresses, or both address types. In order to use this service to map domain names to IPv6 addresses, you must specify a name server and enable the DNS, which is the global naming scheme of the Internet that uniquely identifies network devices.

Cisco software maintains a cache of hostname-to-address mappings for use by the **connect**, **telnet**, and **ping** commands, related Telnet support operations, and many other commands that generate command output. This cache speeds the conversion of names to addresses.

Similar to IPv4, IPv6 uses a naming scheme that allows a network device to be identified by its location within a hierarchical name space that provides for domains. Domain names are joined with periods (.) as the delimiting characters. For example, Cisco is a commercial organization that is identified by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, the FTP server, for example, is identified as *ftp.cisco.com*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 host name [port] ipv6-address1 [ipv6-address2...ipv6-address4]**
4. Do one of the following:
 - **ip domain name [vrf vrf-name] name**
 -
 -
 - **ip domain list [vrf vrf-name] name**
5. **ip name-server [vrf vrf-name] server-address1 [server-address2...server-address6]**
6. **ip domain-lookup**

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 enable</p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
<p>Step 2 configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p>Step 3 ipv6 host name [port] ipv6-address1 [ipv6-address2...ipv6-address4]</p> <p>Example:</p> <pre>Device(config)# ipv6 host cisco-sj 2001:DB8:20:1::12</pre>	<p>Defines a static hostname-to-address mapping in the hostname cache.</p> <ul style="list-style-type: none"> Typically, it is easier to refer to network devices by symbolic names rather than numerical addresses (services such as Telnet can use hostnames or addresses). Hostnames and IPv6 addresses can be associated with one another through static or dynamic means. Manually assigning hostnames to addresses is useful when dynamic mapping is not available.
<p>Step 4 Do one of the following:</p> <ul style="list-style-type: none"> ip domain name [vrf vrf-name] name ip domain list [vrf vrf-name] name <p>Example:</p> <pre>Device(config)# ip domain-name cisco.com</pre> <p>Example:</p> <pre>Device(config)# ip domain list cisco1.com</pre>	<p>(Optional) Defines a default domain name that Cisco software will use to complete unqualified hostnames.</p> <p>or</p> <p>(Optional) Defines a list of default domain names to complete unqualified hostnames.</p> <ul style="list-style-type: none"> You can specify a default domain name that Cisco software will use to complete domain name requests. You can specify either a single domain name or a list of domain names. Any hostname that does not contain a complete domain name will have the default domain name you specify appended to it before the name is looked up. <p>Note The ip domain name and ip domain list commands are used to specify default domain names that can be used by both IPv4 and IPv6.</p>

Command or Action	Purpose
Step 5 ip name-server [<i>vrf vrf-name</i>] <i>server-address1</i> [<i>server-address2...server-address6</i>] Example: <pre>Device(config)# ip name-server 2001:DB8::250:8bff:fee8:f800 2001:DB8:0:f004::1</pre>	Specifies one or more hosts that supply name information. <ul style="list-style-type: none"> Specifies one or more hosts (up to six) that can function as a name server to supply name information for DNS. Note The <i>server-address</i> argument can be either an IPv4 or IPv6 address.
Step 6 ip domain-lookup Example: <pre>Device(config)# ip domain-lookup</pre>	Enables DNS-based address translation. <ul style="list-style-type: none"> DNS is enabled by default.

Displaying IPv6 Redirect Messages

SUMMARY STEPS

1. enable
2. show ipv6 interface [*brief*] [*type number*] [*prefix*]
3. show ipv6 neighbors [*interface-type interface-number* | *ipv6-address* | *ipv6-hostname*] **statistics**
4. show ipv6 route [*ipv6-address* | *ipv6-prefix/prefix-length* | *protocol* | *interface-type interface-number*]
5. show ipv6 traffic
6. show hosts [*vrf vrf-name* | **all** | *hostname* | **summary**]
7. enable
8. show running-config

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: <pre>Device# enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 show ipv6 interface [<i>brief</i>] [<i>type number</i>] [<i>prefix</i>] Example: <pre>Device# show ipv6 interface gigabitethernet 0/0/0</pre>	Displays the usability status of interfaces configured for IPv6.

Command or Action	Purpose
Step 3 show ipv6 neighbors [<i>interface-type interface-number</i> <i>ipv6-address</i> <i>ipv6-hostname</i>] statistics Example: Device# show ipv6 neighbors gigabitethernet 2/0/0	Displays IPv6 Neighbor Discovery cache information.
Step 4 show ipv6 route [<i>ipv6-address</i> <i>ipv6-prefix/prefix-length</i> <i>protocol</i> <i>interface-type interface-number</i>] Example: Device# show ipv6 route	(Optional) Displays the current contents of the IPv6 routing table.
Step 5 show ipv6 traffic Example: Device# show ipv6 traffic	(Optional) Displays statistics about IPv6 traffic.
Step 6 show hosts [<i>vrf vrf-name</i> all <i>hostname</i> summary] Example: Device# show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.
Step 7 enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 8 show running-config Example: Device# show running-config	Displays the current configuration running on the device.

Configuration Examples for IPv6 Addressing and Basic Connectivity

- [Example: IPv6 Addressing and IPv6 Routing Configuration, page 18](#)
- [Example: Dual-Protocol Stacks Configuration, page 18](#)

- [Example: Hostname-to-Address Mappings Configuration, page 18](#)

Example: IPv6 Addressing and IPv6 Routing Configuration

In the following example, IPv6 is enabled on the device with both a link-local address and a global address based on the IPv6 prefix 2001:DB8:C18:1::/64. The EUI-64 interface ID is used in the low-order 64 bits of both addresses. Output from the **show ipv6 interface** command is included to show how the interface ID (260:3EFF:FE47:1530) is appended to the link-local prefix FE80::/64 of Gigabit Ethernet interface 0/0/0.

```
ipv6 unicast-routing
interface gigabitethernet 0/0/0
  ipv6 address 2001:DB8:C18:1::/64 eui-64
Device# show ipv6 interface gigabitethernet 0/0/0
Gigabitethernet0/0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::260:3EFF:FE47:1530
Global unicast address(es):
  2001:DB8:C18:1:260:3EFF:FE47:1530, subnet is 2001:DB8:C18:1::/64
Joined group address(es):
  FE02::1
  FE02::2
  FE02::1:FF47:1530
  FE02::9
MTU is 1500 bytes
ICMP error messages limited to one every 500 milliseconds
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.
```

Example: Dual-Protocol Stacks Configuration

The following example enables the forwarding of IPv6 unicast datagrams globally on the device and configures Gigabit Ethernet interface 0/0/0 with both an IPv4 address and an IPv6 address:

```
ipv6 unicast-routing
interface gigabitethernet0/0/0
  ip address 192.168.99.1 255.255.255.0
  ipv6 address 2001:DB8:C18:1::3/64
```

Example: Hostname-to-Address Mappings Configuration

The following example defines two static hostname-to-address mappings in the hostname cache, establishes a domain list with several alternate domain names to complete unqualified hostnames, specifies host 2001:DB8::250:8bff:fee8:f800 and host 2001:DB8:0:f004::1 as the name servers, and reenables the DNS service:

```
ipv6 host cisco-sj 2001:DB8:700:20:1::12
ipv6 host cisco-hq 2001:DB8:768::1 2001:DB8:20:1::22
ip domain list domain1-list.com
ip domain list serviceprovider2-name.com
ip domain list college2-name.edu
ip name-server 2001:DB8::250:8bff:fee8:f800 2001:DB8:0:f004::1
ip domain-lookup
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
IPv4 addressing	<i>IP Addressing: IPv4 Addressing Configuration Guide</i>
IPv4 services configuration tasks	<i>IP Application Services Configuration Guide</i>
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

MIBs

MIB	MIBs Link
	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Addressing and Basic Connectivity

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5 *Feature Information for IPv6 Addressing and Basic Connectivity*

Feature Name	Releases	Feature Information
Internet Protocol version 6 (IPv6)	12.0(22)S	IPv6 expands the number of network address bits from 32 bits to 128 bits, which provides more than enough globally unique IP addresses for every networked device on the planet.
	12.2(2)T	
	12.2(14)S	
	12.2(17a)SX1	
	12.2(25)SEA	
	12.2(28)SB	
	12.2(33)SRA	
	Cisco IOS XE Release 2.1	The following commands were introduced or modified: ip address , ip domain list , ip domain-lookup ip domain name , ip name-server , ipv6 address , ipv6 address anycast , ipv6 address eui-64 , ipv6 address link-local , ipv6 enable , ipv6 host , ipv6 unicast-routing .
IPv6 Data Link: VLANs using Cisco Inter-Switch Link	12.2(2)T	IPv6 supports this feature.
	12.2(18)SXE	
	12.2(25)SEA	
	12.2(25)SG	
	12.2(33)SRA	
	15.0(2)SG	
	3.2.0SG	No commands were introduced or modified.

Feature Name	Releases	Feature Information
IPv6 Data Link: VLANs Using IEEE 802.1Q Encapsulation	12.2(2)T	IPv6 supports this feature. No commands were introduced or modified.
	12.2(18)SXE	
	12.2(25)SEA	
	12.2(25)SG	
	12.2(33)SRA	
	15.0(2)SG	
	3.2.0SG	
IPv6 Services: Cisco Discovery Protocol—IPv6 Address Family Support for Neighbor Information	12.2(8)T	The Cisco Discovery Protocol—IPv6 Address Support for Neighbor Information feature adds the ability to transfer IPv6 addressing information between two Cisco devices. No commands were introduced or modified.
	12.2(14)S	
	12.2(18)SXE	
	12.2(25)SEE	
	12.2(25)SG	
	12.2(33)SRA	
	Cisco IOS XE Release 2.1	

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



IPv6 Anycast Address

An IPv6 anycast address is an address that is assigned to a set of interfaces that typically belong to different nodes. Anycast addresses are syntactically indistinguishable from unicast addresses, because anycast addresses are allocated from the unicast address space.

- [Finding Feature Information, page 23](#)
- [Information About IPv6 Anycast Address, page 23](#)
- [How to Configure IPv6 Anycast Address, page 24](#)
- [Configuration Examples for IPv6 Anycast Address, page 25](#)
- [Additional References, page 26](#)
- [Feature Information for IPv6 Anycast Address, page 27](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPv6 Anycast Address

- [IPv6 Address Type: Anycast, page 23](#)

IPv6 Address Type: Anycast

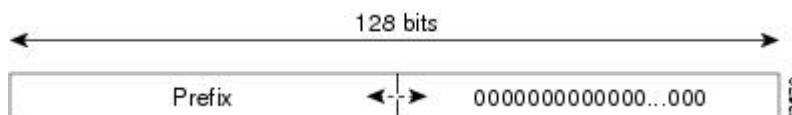
An anycast address is an address that is assigned to a set of interfaces that typically belong to different nodes. A packet sent to an anycast address is delivered to the closest interface (as defined by the routing protocols in use) identified by the anycast address. Anycast addresses are syntactically indistinguishable from unicast addresses, because anycast addresses are allocated from the unicast address space. Assigning a unicast address to more than one interface makes a unicast address an anycast address. Nodes to which the anycast address is assigned must be explicitly configured to recognize that the address is an anycast address.

**Note**

Anycast addresses can be used only by a device, not a host, and anycast addresses must not be used as the source address of an IPv6 packet.

The figure below shows the format of the subnet device anycast address; the address has a prefix concatenated by a series of zeros (the interface ID). The subnet device anycast address can be used to reach a device on the link that is identified by the prefix in the subnet device anycast address.

Figure 8 Subnet Device Anycast Address Format



How to Configure IPv6 Anycast Address

- [Configuring IPv6 Anycast Addressing, page 24](#)

Configuring IPv6 Anycast Addressing

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *type number***
4. **tunnel mode ipv6ip [6rd | 6to4 | auto-tunnel | isatap]**
5. **tunnel source { *ip address* | *ipv6-address* | *interface-type interface-number* }**
6. **ipv6 address { *ipv6-prefix/prefix-length* | *prefix-name sub-bits/prefix-length* }**
7. **ipv6 address *ipv6-prefix/prefix-length* anycast**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface type number Example: Device(config)# interface tunnel0	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	tunnel mode ipv6ip [6rd 6to4 auto-tunnel isatap] Example: Device(config-if)# tunnel mode ipv6ip 6to4	Configures a static IPv6 tunnel interface.
Step 5	tunnel source { ip address ipv6-address interface-type interface-number } Example: Device(config-if)# tunnel source GigabitEthernet1	Sets the source address for a tunnel interface. The address used here is the one assigned to Ethernet interface 1.
Step 6	ipv6 address { ipv6-prefix/prefix-length prefix-name sub-bits/prefix-length } Example: Device(config-if)# ipv6 address 2001:db8:A00:1::1/64	Configures an IPv6 address and enables IPv6 processing on an interface.
Step 7	ipv6 address ipv6-prefix/prefix-length anycast Example: Device(config-if)# ipv6 address 2002:db8:c058::/128 anycast	Specifying the ipv6 address anycast command adds an IPv6 anycast address.

Configuration Examples for IPv6 Anycast Address

- [Example: Configuring IPv6 Anycast Addressing, page 25](#)

Example: Configuring IPv6 Anycast Addressing

```
interface tunnel0
 tunnel mode ipv6ip 6to4
```

```

tunnel source ethernet1
ipv6 address 2001:0db8:1::1/64
ipv6 address 2002:0db8:6301::/128 anycast
!
interface gigabitethernet1
ip address 10.0.0.1 255.255.255.0
ip address 192.88.99.1 255.255.255.0 secondary

```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
IPv4 addressing	<i>IP Addressing: IPv4 Addressing Configuration Guide</i>
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Anycast Address

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 6 Feature Information for IPv6 Anycast Address

Feature Name	Releases	Feature Information
IPv6: Anycast Address	12.2(25)SEA	An anycast address is an address that is assigned to a set of interfaces that typically belong to different nodes. Anycast addresses are syntactically indistinguishable from unicast addresses, because anycast addresses are allocated from the unicast address space.
	12.2(25)SG	
	12.2(33)SRA	
	12.2(33)SXH	
	12.3(4)T	
	15.0(2)SG	
	Cisco IOS XE Release 2.1 3.2.0SG	The following commands were introduced or modified: ipv6 address anycast , show ipv6 interface .

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams,

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support

The Cisco Express Forwarding feature is Layer 3 IP switching technology for the forwarding of IPv6 packets. Distributed Cisco Express Forwarding performs the same functions as Cisco Express Forwarding but for distributed architecture platforms.

- [Finding Feature Information, page 29](#)
- [Prerequisites for IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support, page 29](#)
- [Information About IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support, page 30](#)
- [How to Configure IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support, page 31](#)
- [Configuration Examples for IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support, page 32](#)
- [Additional References, page 33](#)
- [Feature Information for IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support, page 34](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support

- To forward IPv6 traffic using Cisco Express Forwarding or distributed Cisco Express Forwarding, you must configure forwarding of IPv6 unicast datagrams globally on the device, and you must configure an IPv6 address on an interface.

- You must enable Cisco Express Forwarding for IPv4 globally on the device before enabling Cisco Express Forwarding for IPv6 globally on the device.
- On distributed architecture platforms that support both Cisco Express Forwarding and distributed Cisco Express Forwarding, you must enable distributed Cisco Express Forwarding for IPv4 globally on the device before enabling distributed Cisco Express Forwarding for IPv6 globally on the device.
- Nondistributed platforms do not support distributed Cisco Express Forwarding; however, some distributed platforms support both Cisco Express Forwarding and distributed Cisco Express Forwarding.
- To use Unicast Reverse Path Forwarding (uRPF), enable Cisco Express Forwarding switching or distributed Cisco Express Forwarding switching in the device. There is no need to configure the input interface for Cisco Express Forwarding switching. As long as Cisco Express Forwarding is running on the device, individual interfaces can be configured with other switching modes.

The following restrictions apply to nondistributed and distributed architecture platforms configured for Cisco Express Forwarding and distributed Cisco Express Forwarding:

- IPv6 packets that have global source and destination addresses are Cisco Express Forwarding-switched or distributed Cisco Express Forwarding-switched.
- IPv6 packets that have link-local source and destination addresses are process-switched.
- IPv6 packets that are tunneled within manually configured IPv6 tunnels are Cisco Express Forwarding-switched.

Information About IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support

- [Cisco Express Forwarding and Distributed Cisco Express Forwarding Switching for IPv6, page 30](#)

Cisco Express Forwarding and Distributed Cisco Express Forwarding Switching for IPv6

Cisco Express Forwarding is advanced, Layer 3 IP switching technology for the forwarding of IPv6 packets. Distributed Cisco Express Forwarding performs the same functions as Cisco Express Forwarding but for distributed architecture platforms. Distributed Cisco Express Forwarding for IPv6 and Cisco Express Forwarding for IPv6 function the same and offer the same benefits as for distributed Cisco Express Forwarding for IPv4 and Cisco Express Forwarding for IPv4. Both have network entries that are added, removed, or modified in the IPv6 Routing Information Base (RIB) (as dictated by the routing protocols in use) and are reflected in the Forwarding Information Bases (FIBs), and the IPv6 adjacency tables maintain Layer 2 next-hop addresses for all entries in each FIB.

Each IPv6 device interface has an association to one IPv6 global FIB and one IPv6 link-local FIB (multiple interfaces can have an association to the same FIB). All IPv6 device interfaces that are attached to the same IPv6 link share the same IPv6 link-local FIB. IPv6 packets that have an IPv6 global destination address are processed by the IPv6 global FIB; however, packets that have an IPv6 global destination address and an IPv6 link-local source address are sent to the Route Processor (RP) for process switching and scope-error handling. Packets that have a link-local source address are not forwarded off of the local link and are sent to the RP for process switching and scope-error handling.

How to Configure IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support

- [Configuring Cisco Express Forwarding Switching on Distributed and Nondistributed Architecture Platforms, page 31](#)

Configuring Cisco Express Forwarding Switching on Distributed and Nondistributed Architecture Platforms

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
 - **ipv6 cef**
 - **ipv6 cef distributed**
4. **ipv6 cef accounting [non-recursive | per-prefix | prefix-length]**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.

Command or Action	Purpose
Step 3 Do one of the following: <ul style="list-style-type: none"> • ipv6 cef • ipv6 cef distributed <p>Example:</p> <pre>Device(config)# ipv6 cef</pre> <p>Example:</p> <pre>Device(config)# ipv6 cef distributed</pre>	Enables Cisco Express Forwarding globally on the device. or Enables distributed Cisco Express Forwarding globally on the device.
Step 4 ipv6 cef accounting [non-recursive per-prefix prefix-length] <p>Example:</p> <pre>Device(config)# ipv6 cef accounting</pre>	Enables Cisco Express Forwarding and distributed Cisco Express Forwarding network accounting globally on the device. <ul style="list-style-type: none"> • Network accounting for Cisco Express Forwarding and distributed Cisco Express Forwarding enables you to better understand Cisco Express Forwarding traffic patterns within your network by collecting statistics specific to Cisco Express Forwarding and distributed Cisco Express Forwarding traffic. For example, network accounting for Cisco Express Forwarding and distributed Cisco Express Forwarding enables you to collect information such as the number of packets and bytes switched to a destination or the number of packets switched through a destination. • The optional per-prefix keyword enables the collection of the number of packets and bytes express forwarded to an IPv6 destination (or IPv6 prefix). • The optional prefix-length keyword enables the collection of the number of packets and bytes express forwarded to an IPv6 prefix length. <p>Note When Cisco Express Forwarding is enabled globally on the device, accounting information is collected at the RP; when distributed Cisco Express Forwarding is enabled globally on the device, accounting information is collected at the line cards.</p>

Configuration Examples for IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support

- [Example: Cisco Express Forwarding and Distributed Cisco Express Forwarding Configuration, page 33](#)

Example: Cisco Express Forwarding and Distributed Cisco Express Forwarding Configuration

In the following example, both Cisco Express Forwarding for IPv6 and network accounting for Cisco Express Forwarding for IPv6 have been enabled globally on a nondistributed architecture device, and Cisco Express Forwarding for IPv6 has been enabled on Gigabit Ethernet interface 0/0/0. The example also shows that the forwarding of IPv6 unicast datagrams has been configured globally on the device with the **ipv6 unicast-routing** command, an IPv6 address has been configured on Gigabit Ethernet interface 0/0/0 with the **ipv6 address** command, and Cisco Express Forwarding for IPv4 has been configured globally on the device with the **ip cef** command.

```
ip cef
ipv6 unicast-routing
ipv6 cef
ipv6 cef accounting prefix-length
interface gigabitethernet0/0/0
 ip address 10.4.9.11 255.0.0.0
 media-type 10BaseT
 ipv6 address 2001:DB8:C18:1::/64 eui-64
```

In the following example, both distributed Cisco Express Forwarding for IPv6 and network accounting for distributed Cisco Express Forwarding for IPv6 have been enabled globally on a distributed architecture device. The forwarding of IPv6 unicast datagrams has been configured globally on the device with the **ipv6 unicast-routing** command and distributed Cisco Express Forwarding for IPv4 has been configured globally on the device with the **ip cef distributed** command.

```
ip cef distributed
ipv6 unicast-routing
ipv6 cef distributed
ipv6 cef accounting prefix-length
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
IPv4 switching configuration	<i>IP Switching Cisco Express Forwarding Configuration Guide</i>
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 7 **Feature Information for IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support**

Feature Name	Releases	Feature Information
IPv6 Switching: Cisco Express Forwarding and Distributed Cisco Express Forwarding Support	12.2(13)T	Cisco Express Forwarding for IPv6 is advanced, Layer 3 IP switching technology for the forwarding of IPv6 packets. Distributed Cisco Express Forwarding for IPv6 performs the same functions as Cisco Express Forwarding for IPv6 but for distributed architecture platforms.
	12.2(17a)SX1	
	12.2(25)SEA	
	12.2(25)SG	
	12.2(33)SRA	
	15.0(2)SG	
	Cisco IOS XE Release 2.1	The following commands were introduced or modified: ipv6 cef , ipv6 cef accounting , ipv6 cef distributed .
	3.2.0SG	

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



Unicast Reverse Path Forwarding for IPv6

The Unicast Reverse Path Forwarding for IPv6 feature mitigates problems caused by malformed or forged (spoofed) IPv6 source addresses that pass through an IPv6 device.

- [Finding Feature Information, page 37](#)
- [Prerequisites for Unicast Reverse Path Forwarding for IPv6, page 37](#)
- [Information About Unicast Reverse Path Forwarding for IPv6, page 38](#)
- [How to Configure Unicast Reverse Path Forwarding for IPv6, page 38](#)
- [Configuration Examples for Unicast Reverse Path Forwarding for IPv6, page 40](#)
- [Additional References, page 40](#)
- [Feature Information for Unicast Reverse Path Forwarding for IPv6, page 41](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Unicast Reverse Path Forwarding for IPv6

- To use Unicast Reverse Path Forwarding (uRPF), enable Cisco Express Forwarding switching or distributed Cisco Express Forwarding switching in the device. There is no need to configure the input interface for Cisco Express Forwarding switching. As long as Cisco Express Forwarding is running on the device, individual interfaces can be configured with other switching modes.
- For uRPF to work, Cisco Express Forwarding must be configured globally in the device. uRPF will not work without Cisco Express Forwarding.
- uRPF 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. uRPF should be applied only where there is natural or configured symmetry.

For example, devices at the edge of the network of an ISP are more likely to have symmetrical reverse paths than devices that are in the core of the ISP network. Devices that are in the core of the ISP network have no guarantee that the best forwarding path out of the device will be the path selected for packets returning to the device. Therefore, we do not recommend that you apply uRPF where there is a

chance of asymmetric routing. Place uRPF only at the edge of a network or, for an ISP, at the customer edge of the network.

Information About Unicast Reverse Path Forwarding for IPv6

- [Unicast Reverse Path Forwarding, page 38](#)

Unicast Reverse Path Forwarding

Use the Unicast Reverse Path Forwarding for IPv6 feature to mitigate problems caused by malformed or spoofed IPv6 source addresses that pass through an IPv6 device. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IPv6 address spoofing.

When uRPF is enabled on an interface, the device examines all packets received on that interface. The device verifies that the source address appears in the routing table and matches the interface on which the packet was received. This "look backward" ability is available only when Cisco Express Forwarding is enabled on the device, because the lookup relies on the presence of the Forwarding Information Bases (FIBs). Cisco Express Forwarding generates the FIB as part of its operation.

**Note**

uRPF is an input function and is applied only on the input interface of a device at the upstream end of a connection.

The uRPF feature verifies whether any packet received at a device interface arrives on one of the best return paths to the source of the packet. The feature performs a reverse lookup in the Cisco Express Forwarding table. If uRPF does not find a reverse path for the packet, uRPF can drop or forward the packet, depending on whether an access control list (ACL) is specified. If an ACL is specified, then when (and only when) a packet fails the uRPF check, the ACL is checked to verify if the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Regardless of whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for uRPF drops and in the interface statistics for uRPF.

If no ACL is specified, the device drops the forged or malformed packet immediately and no ACL logging occurs. The device and interface uRPF counters are updated.

uRPF events can be logged by specifying the logging option for the ACL entries. Log information can be used to gather information about the attack, such as source address and time.

**Note**

With uRPF, all equal-cost "best" return paths are considered valid. uRPF 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) and as long as the route is in the FIB.

How to Configure Unicast Reverse Path Forwarding for IPv6

- [Configuring Unicast RPF, page 39](#)

Configuring Unicast RPF

To use uRPF, enable Cisco Express Forwarding switching or distributed Cisco Express Forwarding switching in the device. There is no need to configure the input interface for Cisco Express Forwarding switching. As long as Cisco Express Forwarding is running on the device, individual interfaces can be configured with other switching modes.



Note

Cisco Express Forwarding must be configured globally in the device. uRPF will not work without Cisco Express Forwarding.



Note

uRPF 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. uRPF should be applied only where there is natural or configured symmetry.

For example, devices at the edge of the network of an ISP are more likely to have symmetrical reverse paths than devices that are in the core of the ISP network. Devices that are in the core of the ISP network have no guarantee that the best forwarding path out of the device will be the path selected for packets returning to the device. Therefore, we do not recommend that you apply uRPF where there is a chance of asymmetric routing. It is simplest to place uRPF only at the edge of a network or, for an ISP, at the customer edge of the network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 verify unicast source reachable-via** {*rx* | **any**} [**allow-default**] [**allow-self-ping**] [*access-list-name*]

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.

Command or Action	Purpose
Step 3 <code>interface type number</code> Example: Device(config)# interface gigabitethernet 0/0/0	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4 <code>ipv6 verify unicast source reachable-via {rx any} [allow-default] [allow-self-ping] [access-list-name]</code> Example: Device(config-if)# ipv6 verify unicast source reachable-via any	Verifies that a source address exists in the FIB table and enables uRPF.

Configuration Examples for Unicast Reverse Path Forwarding for IPv6

- [Example: Configuring Unicast Reverse Path Forwarding for IPv6, page 40](#)

Example: Configuring Unicast Reverse Path Forwarding for IPv6

```
Device# show ipv6 traffic
IPv6 statistics:
  Rcvd:  0 total, 0 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
        0 unicast RPF drop, 0 suppressed RPF drop
  Sent:  0 generated, 0 forwarded
        0 fragmented into 0 fragments, 0 failed
        0 encapsulation failed, 0 no route, 0 too big
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
IPv4 switching configuration	<i>IP Switching Cisco Express Forwarding Configuration Guide</i>

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Unicast Reverse Path Forwarding for IPv6

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 8 **Feature Information for Unicast Reverse Path Forwarding for IPv6**

Feature Name	Releases	Feature Information
Unicast Reverse Path Forwarding for IPv6	12.2(50)SY Cisco IOS XE Release 2.1	Use the uRPF feature to mitigate problems caused by malformed or spoofed IPv6 source addresses that pass through an IPv6 device. Malformed or forged source addresses can indicate DoS attacks based on source IPv6 address spoofing. The following commands were introduced or modified: ipv6 verify unicast source reachable-via, show ipv6 traffic.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



IPv6 Services: AAAA DNS Lookups over an IPv4 Transport

IPv6 basic connectivity can be enhanced by configuring support for AAAA record types in the DNS name-to-address and address-to-name lookup processes.

- [Finding Feature Information, page 43](#)
- [Information About IPv6 Services: AAAA DNS Lookups over an IPv4 Transport, page 43](#)
- [Additional References, page 44](#)
- [Feature Information for IPv6 Services: AAAA DNS Lookups over an IPv4 Transport, page 45](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPv6 Services: AAAA DNS Lookups over an IPv4 Transport

- [DNS for IPv6, page 43](#)

DNS for IPv6

IPv6 supports DNS record types that are supported in the DNS name-to-address and address-to-name lookup processes. The DNS record types support IPv6 addresses. IPv6 also supports the reverse mapping of IPv6 addresses to DNS names.

A name server is used to track information associated with domain names. A name server can maintain a database of hostname-to-address mappings. Each name can map to one or more IPv4 addresses, IPv6 addresses, or both address types. In order to use this service to map domain names to IPv6 addresses, you must specify a name server and enable the DNS.

Similar to IPv4, IPv6 uses a naming scheme that allows a network device to be identified by its location within a hierarchical name space that provides for domains. Domain names are joined with periods (.) as the delimiting characters. For example, Cisco is a commercial organization that is identified by a com domain name, so its domain name is cisco.com. A specific device in this domain, the FTP server, for example, is identified as ftp.cisco.com.

Table 9 **IPv6 DNS Record Types**

Record Type	Description	Format
AAAA	Maps a hostname to an IPv6 address. (Equivalent to an A record in IPv4.)	www.abc.test AAAA 3FFE:YYYY:C18:1::2
PTR	Maps an IPv6 address to a hostname. (Equivalent to a pointer record [PTR] in IPv4.) Note Cisco software supports resolution of PTR records for the IP6.INT domain.	2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.8.1. c.0.y.y.y.e.f.f.3.ip6.int PTR www.abc.test

Additional References

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
IPv4 services configuration	<i>IP Application Services Configuration Guide</i>
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

MIBs

MIB	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Services: AAAA DNS Lookups over an IPv4 Transport

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 10 Feature Information for IPv6 Services: AAAA DNS Lookups over an IPv4 Transport

Feature Name	Releases	Feature Information
IPv6 Services: AAAA DNS Lookups over an IPv4 Transport	12.2(2)T	IPv6 basic connectivity can be enhanced by configuring support for AAAA record types in the DNS name-to-address and address-to-name lookup processes.
	12.2(25)SEA	
	12.2(25)SG	
	12.2(33)SRA	
	12.2(17a)SX1	No commands were introduced or modified.
	15.0(2)SG	
	Cisco IOS XE Release 2.1	
	3.2.0SG	

Feature Name	Releases	Feature Information
IPv6 Services: DNS Lookups over an IPv6 Transport	12.2(8)T	IPv6 supports this feature.
	12.2(25)SED	No commands were introduced or modified.
	12.2(25)SG	
	12.2(33)SRA	
	12.2(17a)SX1	
	15.0(2)SG	
	Cisco IOS XE Release 2.1	
	3.2.0SG	

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



IPv6 MTU Path Discovery

IPv6 MTU Path Discovery allows a host to dynamically discover and adjust to differences in the maximum transmission unit (MTU) size of every link along a given data path.

- [Finding Feature Information, page 47](#)
- [Information About IPv6 MTU Path Discovery, page 47](#)
- [How to Configure IPv6 MTU Path Discovery, page 49](#)
- [Configuration Examples for IPv6 MTU Path Discovery, page 50](#)
- [Additional References, page 50](#)
- [Feature Information for IPv6 MTU Path Discovery, page 51](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPv6 MTU Path Discovery

- [IPv6 MTU Path Discovery, page 47](#)
- [ICMP for IPv6, page 48](#)

IPv6 MTU Path Discovery

As in IPv4, path MTU discovery in IPv6 allows a host to dynamically discover and adjust to differences in the MTU size of every link along a given data path. In IPv6, however, fragmentation is handled by the source of a packet when the path MTU of one link along a given data path is not large enough to accommodate the size of the packets. Having IPv6 hosts handle packet fragmentation saves IPv6 device processing resources and helps IPv6 networks run more efficiently.

**Note**

In IPv6, the minimum link MTU is 1280 octets. We recommend using an MTU value of 1500 octets for IPv6 links.

With IPv6 path MTU discovery, a device originating IPv6 traffic has an MTU cache that contains MTU values received in ICMPv6 "toobig" messages. In order to prevent an attacker from filling the MTU cache, the device keeps track of the destinations to which it has originated (sent) traffic, and only accepts toobig ICMPv6 messages that have an inner destination matching one of these tracked destinations.

If a malicious device can learn to which destination the device is originating traffic, it could still send a toobig ICMPv6 message to the device for this destination, even if the attacker is not on the path to this destination, and succeeds in forcing his entry into the MTU cache. The device then starts fragmenting traffic to this destination, which significantly affects device performance.

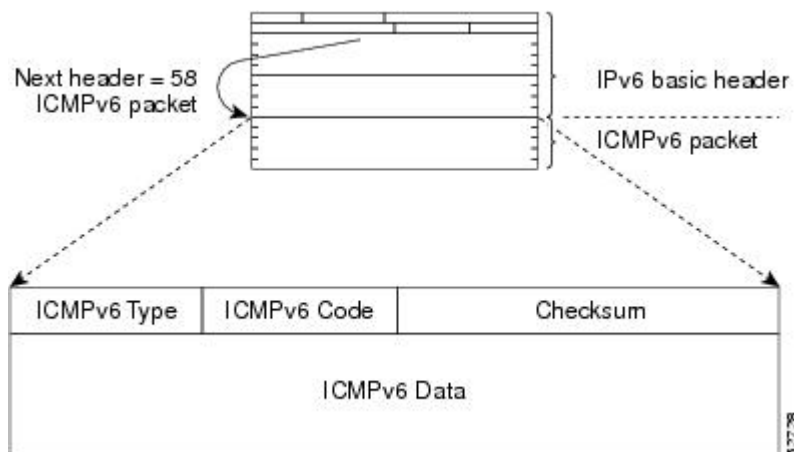
Enabling flow-label marking for locally generated traffic can mitigate this attack. Originated packets are marked with a flow label (which is randomly generated and changed every minute), and toobig messages received are checked against the values sent. Unless an attacker can snoop traffic, the attacker will not know which flow label to use, and its toobig message will be dropped.

ICMP for IPv6

Internet Control Message Protocol (ICMP) in IPv6 functions the same as ICMP in IPv4. ICMP generates error messages, such as ICMP destination unreachable messages, and informational messages, such as ICMP echo request and reply messages. Additionally, ICMP packets in IPv6 are used in the IPv6 neighbor discovery process, path MTU discovery, and the Multicast Listener Discovery (MLD) protocol for IPv6. MLD is used by IPv6 devices to discover multicast listeners (nodes that want to receive multicast packets destined for specific multicast addresses) on directly attached links. MLD is based on version 2 of the Internet Group Management Protocol (IGMP) for IPv4.

A value of 58 in the Next Header field of the basic IPv6 packet header identifies an IPv6 ICMP packet. ICMP packets in IPv6 are like a transport-layer packet in the sense that the ICMP packet follows all the extension headers and is the last piece of information in the IPv6 packet. Within IPv6 ICMP packets, the ICMPv6 Type and ICMPv6 Code fields identify IPv6 ICMP packet specifics, such as the ICMP message type. The value in the Checksum field is derived (computed by the sender and checked by the receiver) from the fields in the IPv6 ICMP packet and the IPv6 pseudoheader. The ICMPv6 Data field contains error or diagnostic information relevant to IP packet processing. The figure below shows the IPv6 ICMP packet header format.

Figure 9 IPv6 ICMP Packet Header Format



How to Configure IPv6 MTU Path Discovery

- [Enabling Flow-Label Marking in Packets that Originate from the Device, page 49](#)

Enabling Flow-Label Marking in Packets that Originate from the Device

This feature allows the device to track destinations to which the device has sent packets that are 1280 bytes or larger.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 flowset**
4. **exit**
5. **clear ipv6 mtu**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ipv6 flowset Example: Device(config)# ipv6 flowset	Configures flow-label marking in 1280-byte or larger packets sent by the device.
Step 4	exit Example: Device(config)# exit	Exits global configuration mode, and places the device in privileged EXEC mode.

Command or Action	Purpose
Step 5 <code>clear ipv6 mtu</code> Example: Device# <code>clear ipv6 mtu</code>	Clears the MTU cache of messages.

Configuration Examples for IPv6 MTU Path Discovery

- [Example: Displaying IPv6 Interface Statistics, page 50](#)

Example: Displaying IPv6 Interface Statistics

In the following example, the **show ipv6 interface** command is used to verify that IPv6 addresses are configured correctly for FastEthernet interface 1/0. Information may also be displayed about the status of IPv6 neighbor redirect messages, IPv6 neighbor discovery messages, stateless autoconfiguration, and MTU size.

```
Device# show ipv6 interface fastethernet 1/0

Ethernet0 is up, line protocol is up
IPv6 is stalled, link-local address is FE80::1
Global unicast address(es):
  2001:DB8:2000::1, subnet is 2001:DB8:2000::/64
  2001:DB8:3000::1, subnet is 2001:DB8:3000::/64
Joined group address(es):
  FE02::1
  FE02::2
  FE02::1:FE00:1
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.
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic		Document Title
IPv6 commands		<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features		Cisco IOS IPv6 Feature Mapping
Standards and RFCs		
Standard/RFC		Title
RFCs for IPv6		<i>IPv6 RFCs</i>
MIBs		
MIB		MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.		To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs
Technical Assistance		
Description		Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.		http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 MTU Path Discovery

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 11 **Feature Information for IPv6 MTU Path Discovery**

Feature Name	Releases	Feature Information
IPv6 MTU Path Discovery	12.2(2)T	Path MTU discovery in IPv6 allows a host to dynamically discover and adjust to differences in the MTU size of every link along a given data path.
	12.2(17a)SX1	
	12.2(25)SEA	
	12.2(25)SG	
	12.2(33)SRA	The following commands were introduced or modified: clear ipv6 mtu , ipv6 flowset .
	15.0(2)SG	
	Cisco IOS XE Release 2.1	
	3.2.0SG	

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



ICMP for IPv6

ICMP in IPv6 functions the same as ICMP in IPv4. ICMP for IPv6 generates error messages, such as ICMP destination unreachable messages, and informational messages, such as ICMP echo request and reply messages.

- [Finding Feature Information, page 53](#)
- [Information About ICMP for IPv6, page 53](#)
- [Additional References, page 57](#)
- [Feature Information for ICMP for IPv6, page 58](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About ICMP for IPv6

- [ICMP for IPv6, page 53](#)

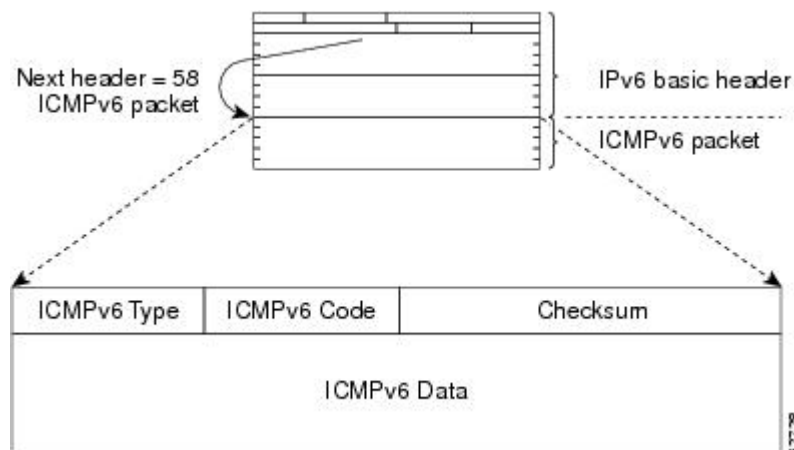
ICMP for IPv6

Internet Control Message Protocol (ICMP) in IPv6 functions the same as ICMP in IPv4. ICMP generates error messages, such as ICMP destination unreachable messages, and informational messages, such as ICMP echo request and reply messages. Additionally, ICMP packets in IPv6 are used in the IPv6 neighbor discovery process, path MTU discovery, and the Multicast Listener Discovery (MLD) protocol for IPv6. MLD is used by IPv6 devices to discover multicast listeners (nodes that want to receive multicast packets destined for specific multicast addresses) on directly attached links. MLD is based on version 2 of the Internet Group Management Protocol (IGMP) for IPv4.

A value of 58 in the Next Header field of the basic IPv6 packet header identifies an IPv6 ICMP packet. ICMP packets in IPv6 are like a transport-layer packet in the sense that the ICMP packet follows all the extension headers and is the last piece of information in the IPv6 packet. Within IPv6 ICMP packets, the ICMPv6 Type and ICMPv6 Code fields identify IPv6 ICMP packet specifics, such as the ICMP message type. The value in the Checksum field is derived (computed by the sender and checked by the receiver)

from the fields in the IPv6 ICMP packet and the IPv6 pseudoheader. The ICMPv6 Data field contains error or diagnostic information relevant to IP packet processing. The figure below shows the IPv6 ICMP packet header format.

Figure 10 IPv6 ICMP Packet Header Format

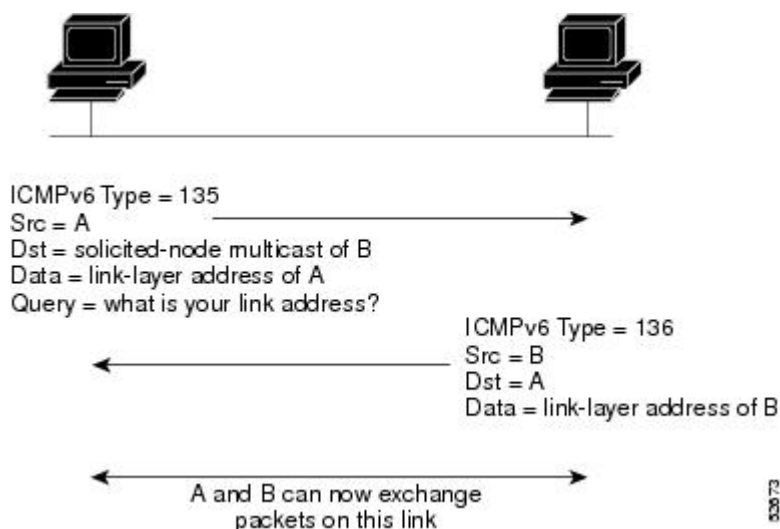


- [IPv6 Neighbor Solicitation Message, page 54](#)
- [IPv6 Router Advertisement Message, page 56](#)

IPv6 Neighbor Solicitation Message

A value of 135 in the Type field of the ICMP packet header identifies a neighbor solicitation message. Neighbor solicitation messages are sent on the local link when a node wants to determine the link-layer address of another node on the same local link (see the figure below). When a node wants to determine the link-layer address of another node, the source address in a neighbor solicitation message is the IPv6 address of the node sending the neighbor solicitation message. The destination address in the neighbor solicitation message is the solicited-node multicast address that corresponds to the IPv6 address of the destination node. The neighbor solicitation message also includes the link-layer address of the source node.

Figure 11 IPv6 Neighbor Discovery: Neighbor Solicitation Message



After receiving the neighbor solicitation message, the destination node replies by sending a neighbor advertisement message, which has a value of 136 in the Type field of the ICMP packet header, on the local link. The source address in the neighbor advertisement message is the IPv6 address of the node (more specifically, the IPv6 address of the node interface) sending the neighbor advertisement message. The destination address in the neighbor advertisement message is the IPv6 address of the node that sent the neighbor solicitation message. The data portion of the neighbor advertisement message includes the link-layer address of the node sending the neighbor advertisement message.

After the source node receives the neighbor advertisement, the source node and destination node can communicate.

Neighbor solicitation messages are also used to verify the reachability of a neighbor after the link-layer address of a neighbor is identified. When a node wants to verify the reachability of a neighbor, the destination address in a neighbor solicitation message is the unicast address of the neighbor.

Neighbor advertisement messages are also sent when there is a change in the link-layer address of a node on a local link. When there is such a change, the destination address for the neighbor advertisement is the all-nodes multicast address.

Neighbor solicitation messages are also used to verify the reachability of a neighbor after the link-layer address of a neighbor is identified. Neighbor unreachability detection identifies the failure of a neighbor or the failure of the forward path to the neighbor, and is used for all paths between hosts and neighboring nodes (hosts or devices). Neighbor unreachability detection is performed for neighbors to which only unicast packets are being sent and is not performed for neighbors to which multicast packets are being sent.

A neighbor is considered reachable when a positive acknowledgment is returned from the neighbor (indicating that packets previously sent to the neighbor have been received and processed). A positive acknowledgment from an upper-layer protocol (such as TCP) indicates that a connection is making forward progress (reaching its destination) or the receipt of a neighbor advertisement message in response to a neighbor solicitation message. If packets are reaching the peer, they are also reaching the next-hop neighbor of the source. Therefore, forward progress is also a confirmation that the next-hop neighbor is reachable.

For destinations that are not on the local link, forward progress implies that the first-hop device is reachable. When acknowledgments from an upper-layer protocol are not available, a node probes the neighbor using unicast neighbor solicitation messages to verify that the forward path is still working.

The return of a solicited neighbor advertisement message from the neighbor is a positive acknowledgment that the forward path is still working (neighbor advertisement messages that have the solicited flag set to a value of 1 are sent only in response to a neighbor solicitation message). Unsolicited messages confirm only the one-way path from the source to the destination node; solicited neighbor advertisement messages indicate that a path is working in both directions.

**Note**

A neighbor advertisement message that has the solicited flag set to a value of 0 must not be considered as a positive acknowledgment that the forward path is still working.

Neighbor solicitation messages are also used in the stateless autoconfiguration process to verify the uniqueness of unicast IPv6 addresses before the addresses are assigned to an interface. Duplicate address detection is performed first on a new, link-local IPv6 address before the address is assigned to an interface (the new address remains in a tentative state while duplicate address detection is performed). Specifically, a node sends a neighbor solicitation message with an unspecified source address and a tentative link-local address in the body of the message. If another node is already using that address, the node returns a neighbor advertisement message that contains the tentative link-local address. If another node is simultaneously verifying the uniqueness of the same address, that node also returns a neighbor solicitation message. If no neighbor advertisement messages are received in response to the neighbor solicitation

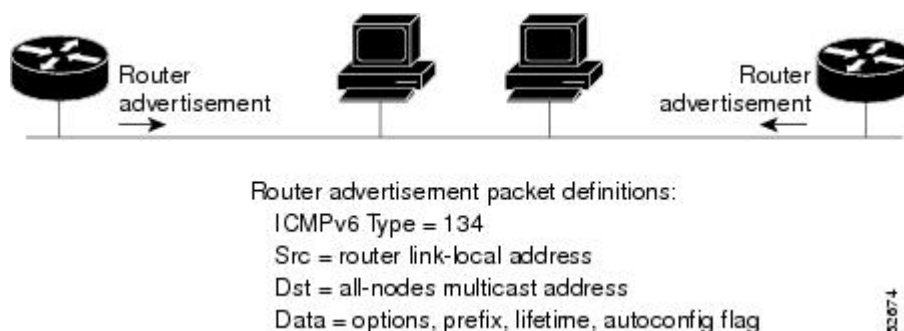
message and no neighbor solicitation messages are received from other nodes that are attempting to verify the same tentative address, the node that sent the original neighbor solicitation message considers the tentative link-local address to be unique and assigns the address to the interface.

Every IPv6 unicast address (global or link-local) must be verified for uniqueness on the link; however, until the uniqueness of the link-local address is verified, duplicate address detection is not performed on any other IPv6 addresses associated with the link-local address. The Cisco implementation of duplicate address detection in the Cisco software does not verify the uniqueness of anycast or global addresses that are generated from 64-bit interface identifiers.

IPv6 Router Advertisement Message

Router advertisement (RA) messages, which have a value of 134 in the Type field of the ICMP packet header, are periodically sent out each configured interface of an IPv6 device. For stateless autoconfiguration to work properly, the advertised prefix length in RA messages must always be 64 bits. The RA messages are sent to the all-nodes multicast address (see the figure below).

Figure 12 IPv6 Neighbor Discovery: RA Message



RA messages typically include the following information:

- One or more onlink IPv6 prefixes that nodes on the local link can use to automatically configure their IPv6 addresses
- Lifetime information for each prefix included in the advertisement
- Sets of flags that indicate the type of autoconfiguration (stateless or stateful) that can be completed
- Default device information (whether the device sending the advertisement should be used as a default device and, if so, the amount of time, in seconds, the device should be used as a default device)
- Additional information for hosts, such as the hop limit and maximum transmission unit (MTU) a host should use in packets that it originates

RAs are also sent in response to device solicitation messages. Device solicitation messages, which have a value of 133 in the Type field of the ICMP packet header, are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled RA message. Given that device solicitation messages are usually sent by hosts at system startup (the host does not have a configured unicast address), the source address in device solicitation messages is usually the unspecified IPv6 address (0:0:0:0:0:0:0:0). If the host has a configured unicast address, the unicast address of the interface sending the device solicitation message is used as the source address in the message. The destination address in device solicitation messages is the all-devices multicast address with a scope of the link. When an RA is sent in response to a device solicitation, the destination address in the RA message is the unicast address of the source of the device solicitation message.

The following RA message parameters can be configured:

- The time interval between periodic RA messages
- The “device lifetime” value, which indicates the usefulness of a device as the default device (for use by all nodes on a given link)
- The network prefixes in use on a given link
- The time interval between neighbor solicitation message retransmissions (on a given link)
- The amount of time a node considers a neighbor reachable (for use by all nodes on a given link)

The configured parameters are specific to an interface. The sending of RA messages (with default values) is automatically enabled on Ethernet and FDDI interfaces when the **ipv6 unicast-routing** command is configured. For other interface types, the sending of RA messages must be manually configured by using the **no ipv6 nd ra suppress** command. The sending of RA messages can be disabled on individual interfaces by using the **ipv6 nd ra suppress** command.

- [Default Router Preferences for Traffic Engineering, page 57](#)

Default Router Preferences for Traffic Engineering

Hosts discover and select default devices by listening to Router Advertisements (RAs). Typical default device selection mechanisms are suboptimal in certain cases, such as when traffic engineering is needed. For example, two devices on a link may provide equivalent but not equal-cost routing, and policy may dictate that one of the devices is preferred. Some examples are as follows:

- Multiple devices that route to distinct sets of prefixes—Redirects (sent by nonoptimal devices for a destination) mean that hosts can choose any device and the system will work. However, traffic patterns may mean that choosing one of the devices would lead to considerably fewer redirects.
- Accidentally deploying a new device—Deploying a new device before it has been fully configured could lead to hosts adopting the new device as a default device and traffic disappearing. Network managers may want to indicate that some devices are more preferred than others.
- Multihomed situations—Multihomed situations may become more common, because of multiple physical links and because of the use of tunneling for IPv6 transport. Some of the devices may not provide full default routing because they route only to the 6-to-4 prefix or they route only to a corporate intranet. These situations cannot be resolved with redirects, which operate only over a single link.

The default router preference (DRP) feature provides a basic preference metric (low, medium, or high) for default devices. The DRP of a default device is signaled in unused bits in RA messages. This extension is backward compatible, both for devices (setting the DRP bits) and hosts (interpreting the DRP bits). These bits are ignored by hosts that do not implement the DRP extension. Similarly, the values sent by devices that do not implement the DRP extension will be interpreted by hosts that do implement it as indicating a “medium” preference. DRPs need to be configured manually.

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ICMP for IPv6

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 12 **Feature Information for ICMP for IPv6**

Feature Name	Releases	Feature Information
IPv6: ICMPv6	12.0(22)S	ICMP in IPv6 functions similarly to ICMP in IPv4. ICMP generates error messages, such as ICMP destination unreachable messages, and informational messages, such as ICMP echo request and reply messages.
	12.2(2)T	
	12.2(14)S	
	12.2(17a)SX1	
	12.2(25)SG	
	12.2(28)SB	No commands were introduced or modified.
	12.2(33)SRA	
	12.2(2)T	
	Cisco IOS XE Release 2.1	

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



IPv6 ICMP Rate Limiting

The IPv6 ICMP rate limiting feature implements a token bucket algorithm for limiting the rate at which IPv6 Internet Control Message Protocol (ICMP) error messages are sent out on the network.

- [Finding Feature Information, page 61](#)
- [Information About IPv6 ICMP Rate Limiting, page 61](#)
- [How to Configure IPv6 ICMP Rate Limiting, page 62](#)
- [Configuration Examples for IPv6 ICMP Rate Limiting, page 63](#)
- [Additional References, page 64](#)
- [Feature Information for IPv6 ICMP Rate Limiting, page 65](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPv6 ICMP Rate Limiting

- [ICMP for IPv6, page 61](#)

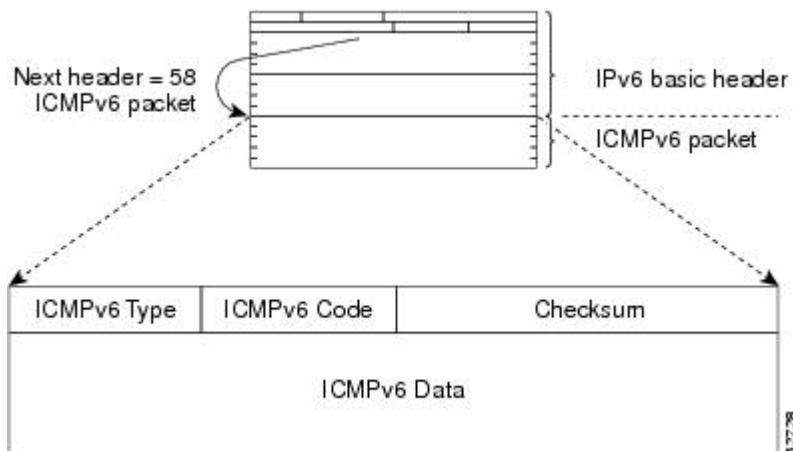
ICMP for IPv6

Internet Control Message Protocol (ICMP) in IPv6 functions the same as ICMP in IPv4. ICMP generates error messages, such as ICMP destination unreachable messages, and informational messages, such as ICMP echo request and reply messages. Additionally, ICMP packets in IPv6 are used in the IPv6 neighbor discovery process, path MTU discovery, and the Multicast Listener Discovery (MLD) protocol for IPv6. MLD is used by IPv6 devices to discover multicast listeners (nodes that want to receive multicast packets destined for specific multicast addresses) on directly attached links. MLD is based on version 2 of the Internet Group Management Protocol (IGMP) for IPv4.

A value of 58 in the Next Header field of the basic IPv6 packet header identifies an IPv6 ICMP packet. ICMP packets in IPv6 are like a transport-layer packet in the sense that the ICMP packet follows all the extension headers and is the last piece of information in the IPv6 packet. Within IPv6 ICMP packets, the ICMPv6 Type and ICMPv6 Code fields identify IPv6 ICMP packet specifics, such as the ICMP message

type. The value in the Checksum field is derived (computed by the sender and checked by the receiver) from the fields in the IPv6 ICMP packet and the IPv6 pseudoheader. The ICMPv6 Data field contains error or diagnostic information relevant to IP packet processing. The figure below shows the IPv6 ICMP packet header format.

Figure 13 IPv6 ICMP Packet Header Format



- [IPv6 ICMP Rate Limiting, page 62](#)

IPv6 ICMP Rate Limiting

The IPv6 ICMP rate limiting feature implements a token bucket algorithm for limiting the rate at which IPv6 ICMP error messages are sent out on the network. The initial implementation of IPv6 ICMP rate limiting defined a fixed interval between error messages, but some applications such as traceroute often require replies to a group of requests sent in rapid succession. The fixed interval between error messages is not flexible enough to work with applications such as traceroute and can cause the application to fail.

Implementing a token bucket scheme allows a number of tokens--representing the ability to send one error message each--to be stored in a virtual bucket. The maximum number of tokens allowed in the bucket can be specified, and for every error message to be sent, one token is removed from the bucket. If a series of error messages is generated, error messages can be sent until the bucket is empty. When the bucket is empty of tokens, no IPv6 ICMP error messages are sent until a new token is placed in the bucket. The token bucket algorithm does not increase the average rate limiting time interval, and it is more flexible than the fixed time interval scheme.

How to Configure IPv6 ICMP Rate Limiting

- [Customizing IPv6 ICMP Rate Limiting, page 63](#)

Customizing IPv6 ICMP Rate Limiting

SUMMARY STEPS

1. enable
2. configure terminal
3. `ipv6 icmp error-interval milliseconds [bucketsize]`

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3 <code>ipv6 icmp error-interval milliseconds [bucketsize]</code> Example: Device(config)# ipv6 icmp error-interval 50 20	Customizes the interval and bucket size for IPv6 ICMP error messages.

Configuration Examples for IPv6 ICMP Rate Limiting

- [Example: IPv6 ICMP Rate Limiting Configuration, page 63](#)
- [Example: Displaying Information About ICMP Rate-Limited Counters, page 63](#)

Example: IPv6 ICMP Rate Limiting Configuration

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
```

Example: Displaying Information About ICMP Rate-Limited Counters

In the following example, information about ICMP rate-limited counters is displayed:

```
Device# show ipv6 traffic
```

```

ICMP statistics:
  Rcvd: 188 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
        1 router solicit, 175 router advert, 0 redirects
        0 neighbor solicit, 12 neighbor advert
  Sent: 7376 output, 56 rate-limited
        unreachable: 0 routing, 15 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout, 0 too big
        15 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 7326 router advert, 0 redirects
        2 neighbor solicit, 22 neighbor advert

```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 ICMP Rate Limiting

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 13 Feature Information for IPv6 ICMP Rate Limiting

Feature Name	Releases	Feature Information
IPv6 ICMP Rate Limiting	12.2(8)T Cisco IOS XE Release 2.1	The IPv6 ICMP Rate Limiting feature implements a token bucket algorithm for limiting the rate at which IPv6 ICMP error messages are sent out on the network. The following commands were introduced or modified: ipv6 icmp error-interval .

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



ICMP for IPv6 Redirect

The IPv6 Redirect Messages feature enables a device to send Internet Control Message Protocol (ICMP) IPv6 neighbor redirect messages to inform hosts of better first-hop nodes (devices or hosts) on the path to a destination.

- [Finding Feature Information, page 67](#)
- [Information About ICMP for IPv6 Redirect, page 67](#)
- [How to Display IPv6 Redirect Messages, page 69](#)
- [Configuration Examples for ICMP for IPv6 Redirect, page 71](#)
- [Additional References, page 71](#)
- [Feature Information for ICMP for IPv6 Redirect, page 72](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About ICMP for IPv6 Redirect

- [ICMP for IPv6, page 67](#)

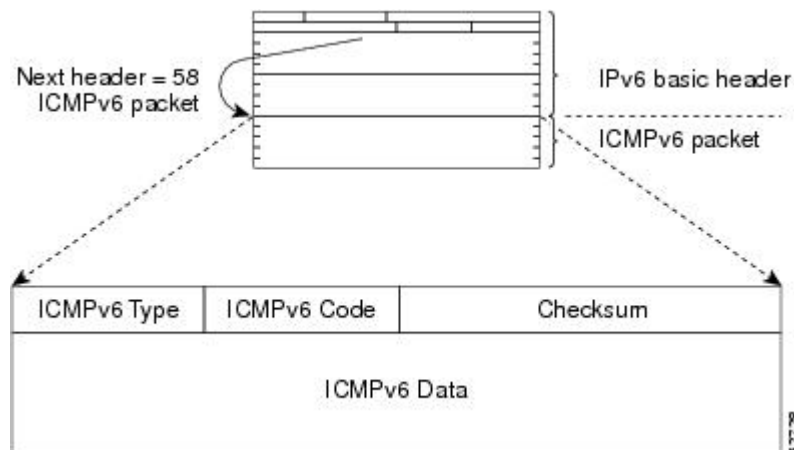
ICMP for IPv6

Internet Control Message Protocol (ICMP) in IPv6 functions the same as ICMP in IPv4. ICMP generates error messages, such as ICMP destination unreachable messages, and informational messages, such as ICMP echo request and reply messages. Additionally, ICMP packets in IPv6 are used in the IPv6 neighbor discovery process, path MTU discovery, and the Multicast Listener Discovery (MLD) protocol for IPv6. MLD is used by IPv6 devices to discover multicast listeners (nodes that want to receive multicast packets destined for specific multicast addresses) on directly attached links. MLD is based on version 2 of the Internet Group Management Protocol (IGMP) for IPv4.

A value of 58 in the Next Header field of the basic IPv6 packet header identifies an IPv6 ICMP packet. ICMP packets in IPv6 are like a transport-layer packet in the sense that the ICMP packet follows all the extension headers and is the last piece of information in the IPv6 packet. Within IPv6 ICMP packets, the

ICMPv6 Type and ICMPv6 Code fields identify IPv6 ICMP packet specifics, such as the ICMP message type. The value in the Checksum field is derived (computed by the sender and checked by the receiver) from the fields in the IPv6 ICMP packet and the IPv6 pseudoheader. The ICMPv6 Data field contains error or diagnostic information relevant to IP packet processing. The figure below shows the IPv6 ICMP packet header format.

Figure 14 IPv6 ICMP Packet Header Format

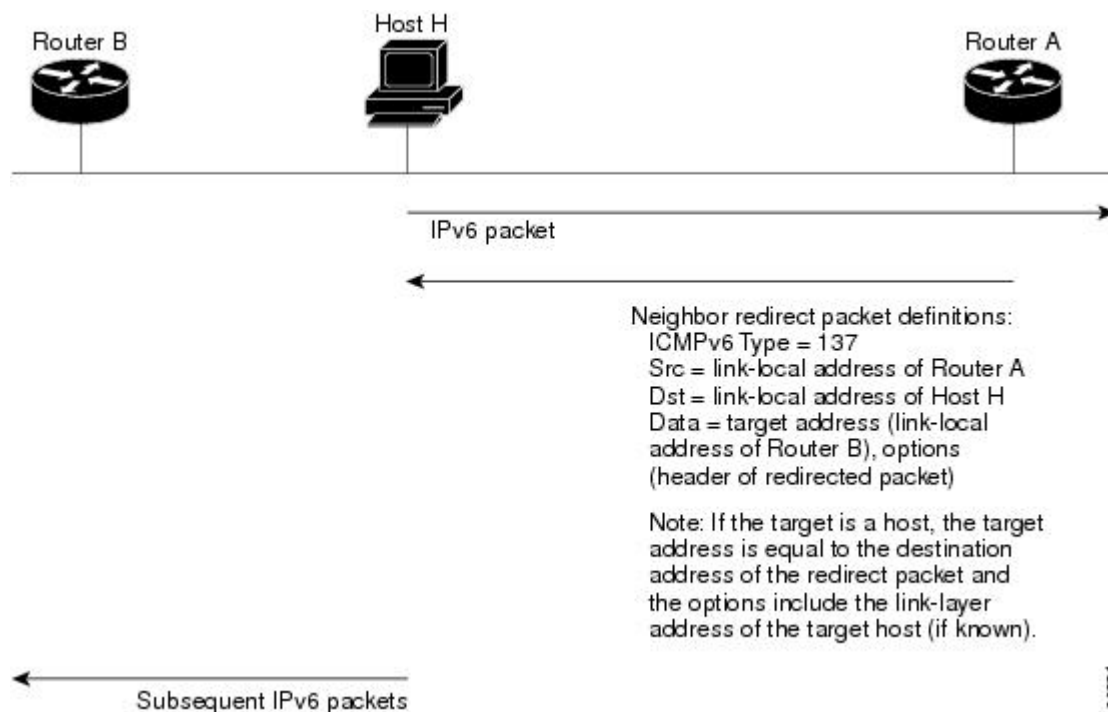


- [IPv6 Neighbor Redirect Message, page 68](#)

IPv6 Neighbor Redirect Message

A value of 137 in the type field of the ICMP packet header identifies an IPv6 neighbor redirect message. Devices send neighbor redirect messages to inform hosts of better first-hop nodes on the path to a destination (see the figure below).

Figure 15 IPv6 Neighbor Discovery: Neighbor Redirect Message



**Note**

A device must be able to determine the link-local address for each of its neighboring devices in order to ensure that the target address (the final destination) in a redirect message identifies the neighbor device by its link-local address. For static routing, the address of the next-hop device should be specified using the link-local address of the device; for dynamic routing, all IPv6 routing protocols must exchange the link-local addresses of neighboring devices.

After forwarding a packet, a device should send a redirect message to the source of the packet under the following circumstances:

- The destination address of the packet is not a multicast address.
- The packet was not addressed to the device.
- The packet is about to be sent out the interface on which it was received.
- The device determines that a better first-hop node for the packet resides on the same link as the source of the packet.
- The source address of the packet is a global IPv6 address of a neighbor on the same link, or a link-local address.

Use the **ipv6 icmp error-interval** command to limit the rate at which the device generates all IPv6 ICMP error messages, including neighbor redirect messages, which ultimately reduces link-layer congestion.

**Note**

A device must not update its routing tables after receiving a neighbor redirect message, and hosts must not originate neighbor redirect messages.

How to Display IPv6 Redirect Messages

- [Displaying IPv6 Redirect Messages, page 69](#)

Displaying IPv6 Redirect Messages

SUMMARY STEPS

1. **enable**
2. **show ipv6 interface** [**brief**] [*type number*] [**prefix**]
3. **show ipv6 neighbors** [*interface-type interface-number* | *ipv6-address* | *ipv6-hostname*] **statistics**
4. **show ipv6 route** [*ipv6-address* | *ipv6-prefix/prefix-length* | *protocol* | *interface-type interface-number*]
5. **show ipv6 traffic**
6. **show hosts** [*vrf vrf-name* | **all** | *hostname* | **summary**]
7. **enable**
8. **show running-config**

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 <code>enable</code></p> <p>Example:</p> <pre>Device# enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
<p>Step 2 <code>show ipv6 interface [brief] [type number] [prefix]</code></p> <p>Example:</p> <pre>Device# show ipv6 interface gigabitethernet 0/0/0</pre>	<p>Displays the usability status of interfaces configured for IPv6.</p>
<p>Step 3 <code>show ipv6 neighbors [interface-type interface-number ipv6-address ipv6-hostname] statistics</code></p> <p>Example:</p> <pre>Device# show ipv6 neighbors gigabitethernet 2/0/0</pre>	<p>Displays IPv6 Neighbor Discovery cache information.</p>
<p>Step 4 <code>show ipv6 route [ipv6-address ipv6-prefix/prefix-length protocol interface-type interface-number]</code></p> <p>Example:</p> <pre>Device# show ipv6 route</pre>	<p>(Optional) Displays the current contents of the IPv6 routing table.</p>
<p>Step 5 <code>show ipv6 traffic</code></p> <p>Example:</p> <pre>Device# show ipv6 traffic</pre>	<p>(Optional) Displays statistics about IPv6 traffic.</p>
<p>Step 6 <code>show hosts [vrf vrf-name all hostname summary]</code></p> <p>Example:</p> <pre>Device# show hosts</pre>	<p>Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.</p>
<p>Step 7 <code>enable</code></p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.

Command or Action	Purpose
Step 8 show running-config Example: Device# show running-config	Displays the current configuration running on the device.

Configuration Examples for ICMP for IPv6 Redirect

- [Example: Displaying IPv6 Interface Statistics, page 71](#)

Example: Displaying IPv6 Interface Statistics

In the following example, the **show ipv6 interface** command is used to verify that IPv6 addresses are configured correctly for GigabitEthernet interface 0/0/0. Information is also displayed about the status of IPv6 neighbor redirect messages, IPv6 neighbor discovery messages, and stateless autoconfiguration.

```
Device# show ipv6 interface gigabitethernet 0/0/0

GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is stalled, link-local address is FE80::1
  Global unicast address(es):
    2001:DB8:2000::1, subnet is 2001:DB8:2000::/64
    2001:DB8:3000::1, subnet is 2001:DB8:3000::/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 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.
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping
Standards and RFCs	
Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>
MIBs	
MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs
Technical Assistance	
Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ICMP for IPv6 Redirect

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 14 **Feature Information for ICMPv for IPv6 Redirect**

Feature Name	Releases	Feature Information
IPv6: ICMPv6 Redirect	12.0(22)S	The IPv6 Redirect Messages feature enables a device to send ICMP IPv6 neighbor redirect messages to inform hosts of better first-hop nodes on the path to a destination.
	12.2(4)T	
	12.2(14)S	
	12.2(17a)SX1	
	12.2(25)SG	The following commands were introduced or modified: show ipv6 interface , show ipv6 neighbors , show ipv6 route , show ipv6 traffic .
	12.2(28)SB	
	12.2(33)SRA	
	Cisco IOS XE Release 2.1	

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



IPv6 Neighbor Discovery

The IPv6 neighbor discovery process uses Internet Control Message Protocol (ICMP) messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and track neighboring devices.

- [Finding Feature Information, page 75](#)
- [Information About IPv6 Neighbor Discovery, page 75](#)
- [How to Configure IPv6 Neighbor Discovery, page 80](#)
- [Configuration Examples for IPv6 Neighbor Discovery, page 84](#)
- [Additional References, page 85](#)
- [Feature Information for IPv6 Neighbor Discovery, page 86](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPv6 Neighbor Discovery

- [IPv6 Neighbor Discovery, page 75](#)

IPv6 Neighbor Discovery

The IPv6 neighbor discovery process uses ICMP messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and track neighboring devices.

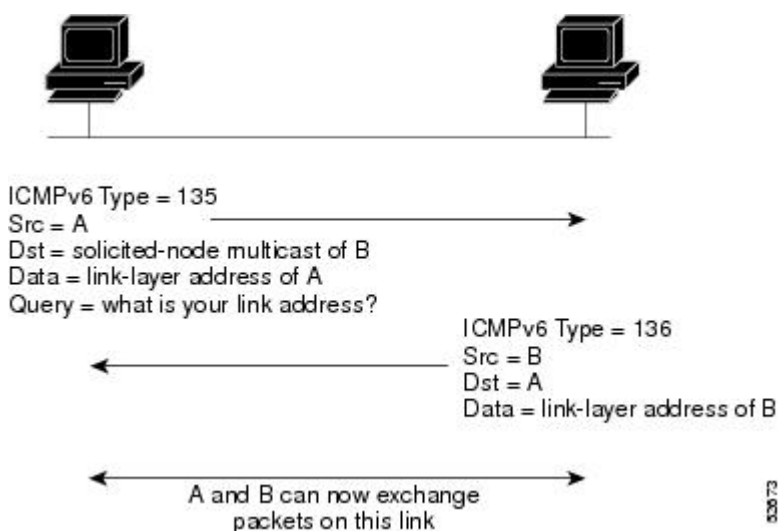
The IPv6 static cache entry for neighbor discovery feature allows static entries to be made in the IPv6 neighbor cache. Static routing requires an administrator to manually enter IPv6 addresses, subnet masks, gateways, and corresponding Media Access Control (MAC) addresses for each interface of each device into a table. Static routing enables more control but requires more work to maintain the table. The table must be updated each time routes are added or changed.

- [IPv6 Neighbor Solicitation Message, page 76](#)
- [IPv6 Router Advertisement Message, page 77](#)
- [IPv6 Neighbor Redirect Message, page 79](#)

IPv6 Neighbor Solicitation Message

A value of 135 in the Type field of the ICMP packet header identifies a neighbor solicitation message. Neighbor solicitation messages are sent on the local link when a node wants to determine the link-layer address of another node on the same local link (see the figure below). When a node wants to determine the link-layer address of another node, the source address in a neighbor solicitation message is the IPv6 address of the node sending the neighbor solicitation message. The destination address in the neighbor solicitation message is the solicited-node multicast address that corresponds to the IPv6 address of the destination node. The neighbor solicitation message also includes the link-layer address of the source node.

Figure 16 IPv6 Neighbor Discovery: Neighbor Solicitation Message



After receiving the neighbor solicitation message, the destination node replies by sending a neighbor advertisement message, which has a value of 136 in the Type field of the ICMP packet header, on the local link. The source address in the neighbor advertisement message is the IPv6 address of the node (more specifically, the IPv6 address of the node interface) sending the neighbor advertisement message. The destination address in the neighbor advertisement message is the IPv6 address of the node that sent the neighbor solicitation message. The data portion of the neighbor advertisement message includes the link-layer address of the node sending the neighbor advertisement message.

After the source node receives the neighbor advertisement, the source node and destination node can communicate.

Neighbor solicitation messages are also used to verify the reachability of a neighbor after the link-layer address of a neighbor is identified. When a node wants to verify the reachability of a neighbor, the destination address in a neighbor solicitation message is the unicast address of the neighbor.

Neighbor advertisement messages are also sent when there is a change in the link-layer address of a node on a local link. When there is such a change, the destination address for the neighbor advertisement is the all-nodes multicast address.

Neighbor solicitation messages are also used to verify the reachability of a neighbor after the link-layer address of a neighbor is identified. Neighbor unreachability detection identifies the failure of a neighbor or

the failure of the forward path to the neighbor, and is used for all paths between hosts and neighboring nodes (hosts or devices). Neighbor unreachability detection is performed for neighbors to which only unicast packets are being sent and is not performed for neighbors to which multicast packets are being sent.

A neighbor is considered reachable when a positive acknowledgment is returned from the neighbor (indicating that packets previously sent to the neighbor have been received and processed). A positive acknowledgment from an upper-layer protocol (such as TCP) indicates that a connection is making forward progress (reaching its destination) or the receipt of a neighbor advertisement message in response to a neighbor solicitation message. If packets are reaching the peer, they are also reaching the next-hop neighbor of the source. Therefore, forward progress is also a confirmation that the next-hop neighbor is reachable.

For destinations that are not on the local link, forward progress implies that the first-hop device is reachable. When acknowledgments from an upper-layer protocol are not available, a node probes the neighbor using unicast neighbor solicitation messages to verify that the forward path is still working.

The return of a solicited neighbor advertisement message from the neighbor is a positive acknowledgment that the forward path is still working (neighbor advertisement messages that have the solicited flag set to a value of 1 are sent only in response to a neighbor solicitation message). Unsolicited messages confirm only the one-way path from the source to the destination node; solicited neighbor advertisement messages indicate that a path is working in both directions.

**Note**

A neighbor advertisement message that has the solicited flag set to a value of 0 must not be considered as a positive acknowledgment that the forward path is still working.

Neighbor solicitation messages are also used in the stateless autoconfiguration process to verify the uniqueness of unicast IPv6 addresses before the addresses are assigned to an interface. Duplicate address detection is performed first on a new, link-local IPv6 address before the address is assigned to an interface (the new address remains in a tentative state while duplicate address detection is performed). Specifically, a node sends a neighbor solicitation message with an unspecified source address and a tentative link-local address in the body of the message. If another node is already using that address, the node returns a neighbor advertisement message that contains the tentative link-local address. If another node is simultaneously verifying the uniqueness of the same address, that node also returns a neighbor solicitation message. If no neighbor advertisement messages are received in response to the neighbor solicitation message and no neighbor solicitation messages are received from other nodes that are attempting to verify the same tentative address, the node that sent the original neighbor solicitation message considers the tentative link-local address to be unique and assigns the address to the interface.

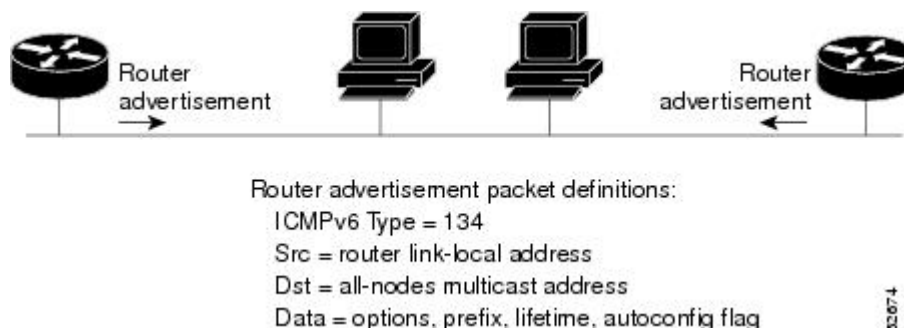
Every IPv6 unicast address (global or link-local) must be verified for uniqueness on the link; however, until the uniqueness of the link-local address is verified, duplicate address detection is not performed on any other IPv6 addresses associated with the link-local address. The Cisco implementation of duplicate address detection in the Cisco software does not verify the uniqueness of anycast or global addresses that are generated from 64-bit interface identifiers.

IPv6 Router Advertisement Message

Router advertisement (RA) messages, which have a value of 134 in the Type field of the ICMP packet header, are periodically sent out each configured interface of an IPv6 device. For stateless autoconfiguration to work properly, the advertised prefix length in RA messages must always be 64 bits.

The RA messages are sent to the all-nodes multicast address (see the figure below).

Figure 17 IPv6 Neighbor Discovery: RA Message



RA messages typically include the following information:

- One or more onlink IPv6 prefixes that nodes on the local link can use to automatically configure their IPv6 addresses
- Lifetime information for each prefix included in the advertisement
- Sets of flags that indicate the type of autoconfiguration (stateless or stateful) that can be completed
- Default device information (whether the device sending the advertisement should be used as a default device and, if so, the amount of time, in seconds, the device should be used as a default device)
- Additional information for hosts, such as the hop limit and maximum transmission unit (MTU) a host should use in packets that it originates

RAs are also sent in response to device solicitation messages. Device solicitation messages, which have a value of 133 in the Type field of the ICMP packet header, are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled RA message. Given that device solicitation messages are usually sent by hosts at system startup (the host does not have a configured unicast address), the source address in device solicitation messages is usually the unspecified IPv6 address (0:0:0:0:0:0:0:0). If the host has a configured unicast address, the unicast address of the interface sending the device solicitation message is used as the source address in the message. The destination address in device solicitation messages is the all-devices multicast address with a scope of the link. When an RA is sent in response to a device solicitation, the destination address in the RA message is the unicast address of the source of the device solicitation message.

The following RA message parameters can be configured:

- The time interval between periodic RA messages
- The “device lifetime” value, which indicates the usefulness of a device as the default device (for use by all nodes on a given link)
- The network prefixes in use on a given link
- The time interval between neighbor solicitation message retransmissions (on a given link)
- The amount of time a node considers a neighbor reachable (for use by all nodes on a given link)

The configured parameters are specific to an interface. The sending of RA messages (with default values) is automatically enabled on Ethernet and FDDI interfaces when the **ipv6 unicast-routing** command is configured. For other interface types, the sending of RA messages must be manually configured by using the **no ipv6 nd ra suppress** command. The sending of RA messages can be disabled on individual interfaces by using the **ipv6 nd ra suppress** command.

- [Default Router Preferences for Traffic Engineering, page 79](#)

Default Router Preferences for Traffic Engineering

Hosts discover and select default devices by listening to Router Advertisements (RAs). Typical default device selection mechanisms are suboptimal in certain cases, such as when traffic engineering is needed. For example, two devices on a link may provide equivalent but not equal-cost routing, and policy may dictate that one of the devices is preferred. Some examples are as follows:

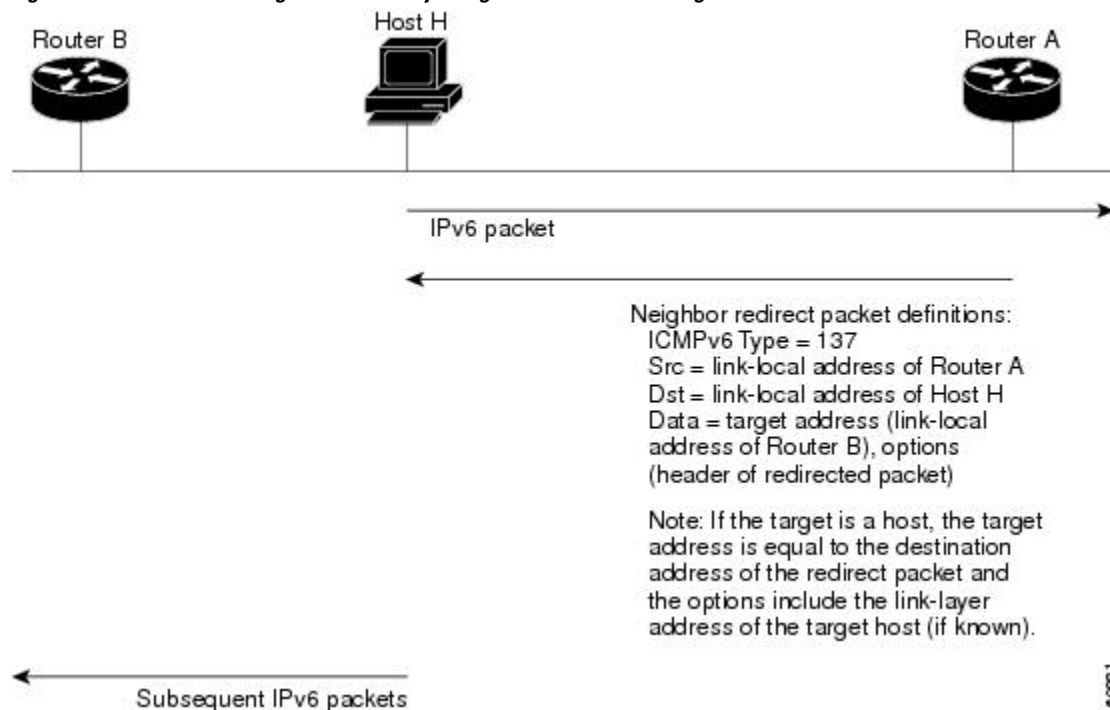
- Multiple devices that route to distinct sets of prefixes—Redirects (sent by nonoptimal devices for a destination) mean that hosts can choose any device and the system will work. However, traffic patterns may mean that choosing one of the devices would lead to considerably fewer redirects.
- Accidentally deploying a new device—Deploying a new device before it has been fully configured could lead to hosts adopting the new device as a default device and traffic disappearing. Network managers may want to indicate that some devices are more preferred than others.
- Multihomed situations—Multihomed situations may become more common, because of multiple physical links and because of the use of tunneling for IPv6 transport. Some of the devices may not provide full default routing because they route only to the 6-to-4 prefix or they route only to a corporate intranet. These situations cannot be resolved with redirects, which operate only over a single link.

The default router preference (DRP) feature provides a basic preference metric (low, medium, or high) for default devices. The DRP of a default device is signaled in unused bits in RA messages. This extension is backward compatible, both for devices (setting the DRP bits) and hosts (interpreting the DRP bits). These bits are ignored by hosts that do not implement the DRP extension. Similarly, the values sent by devices that do not implement the DRP extension will be interpreted by hosts that do implement it as indicating a “medium” preference. DRPs need to be configured manually.

IPv6 Neighbor Redirect Message

A value of 137 in the type field of the ICMP packet header identifies an IPv6 neighbor redirect message. Devices send neighbor redirect messages to inform hosts of better first-hop nodes on the path to a destination (see the figure below).

Figure 18 IPv6 Neighbor Discovery: Neighbor Redirect Message



**Note**

A device must be able to determine the link-local address for each of its neighboring devices in order to ensure that the target address (the final destination) in a redirect message identifies the neighbor device by its link-local address. For static routing, the address of the next-hop device should be specified using the link-local address of the device; for dynamic routing, all IPv6 routing protocols must exchange the link-local addresses of neighboring devices.

After forwarding a packet, a device should send a redirect message to the source of the packet under the following circumstances:

- The destination address of the packet is not a multicast address.
- The packet was not addressed to the device.
- The packet is about to be sent out the interface on which it was received.
- The device determines that a better first-hop node for the packet resides on the same link as the source of the packet.
- The source address of the packet is a global IPv6 address of a neighbor on the same link, or a link-local address.

Use the **ipv6 icmp error-interval** command to limit the rate at which the device generates all IPv6 ICMP error messages, including neighbor redirect messages, which ultimately reduces link-layer congestion.

**Note**

A device must not update its routing tables after receiving a neighbor redirect message, and hosts must not originate neighbor redirect messages.

How to Configure IPv6 Neighbor Discovery

- [Tuning the Parameters for IPv6 Neighbor Discovery, page 80](#)
- [Customizing IPv6 ICMP Rate Limiting, page 81](#)
- [Displaying IPv6 Redirect Messages, page 82](#)

Tuning the Parameters for IPv6 Neighbor Discovery

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *type number***
4. **ipv6 nd nud retry *base interval max-attempts***
5. **ipv6 nd cache expire *expire-time-in-seconds* [refresh]**
6. **ipv6 nd na glean**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 1/0/0	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	ipv6 nd nud retry <i>base interval max-attempts</i> Example: Device(config-if)# ipv6 nd nud retry 1 1000 3	Configures the number of times NUD resends neighbor solicitations.
Step 5	ipv6 nd cache expire <i>expire-time-in-seconds</i> [refresh] Example: Device(config-if)# ipv6 nd cache expire 7200	Configures the length of time before an IPv6 ND cache entry expires.
Step 6	ipv6 nd na glean Example: Device(config-if)# ipv6 nd na glean	Configures ND to glean an entry from an unsolicited NA.

Customizing IPv6 ICMP Rate Limiting

SUMMARY STEPS

1. enable
2. configure terminal
3. ipv6 icmp error-interval *milliseconds* [*bucketsize*]

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3 <code>ipv6 icmp error-interval <i>milliseconds</i> [<i>bucket-size</i>]</code> Example: <pre>Device(config)# ipv6 icmp error-interval 50 20</pre>	Customizes the interval and bucket size for IPv6 ICMP error messages.

Displaying IPv6 Redirect Messages

SUMMARY STEPS

1. `enable`
2. `show ipv6 interface [brief] [type number] [prefix]`
3. `show ipv6 neighbors [interface-type interface-number | ipv6-address | ipv6-hostname] statistics`
4. `show ipv6 route [ipv6-address | ipv6-prefix/prefix-length | protocol | interface-type interface-number]`
5. `show ipv6 traffic`
6. `show hosts [vrf vrf-name | all | hostname | summary]`
7. `enable`
8. `show running-config`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: <pre>Device# enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.

	Command or Action	Purpose
Step 2	show ipv6 interface [brief] [type number] [prefix] Example: Device# show ipv6 interface gigabitethernet 0/0/0	Displays the usability status of interfaces configured for IPv6.
Step 3	show ipv6 neighbors [interface-type interface-number ipv6-address ipv6-hostname] statistics Example: Device# show ipv6 neighbors gigabitethernet 2/0/0	Displays IPv6 Neighbor Discovery cache information.
Step 4	show ipv6 route [ipv6-address ipv6-prefix/prefix-length protocol interface-type interface-number] Example: Device# show ipv6 route	(Optional) Displays the current contents of the IPv6 routing table.
Step 5	show ipv6 traffic Example: Device# show ipv6 traffic	(Optional) Displays statistics about IPv6 traffic.
Step 6	show hosts [vrf vrf-name all hostname summary] Example: Device# show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.
Step 7	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 8	show running-config Example: Device# show running-config	Displays the current configuration running on the device.

Configuration Examples for IPv6 Neighbor Discovery

- [Example: Customizing the Parameters for IPv6 Neighbor Discovery, page 84](#)
- [Example: IPv6 ICMP Rate Limiting Configuration, page 84](#)
- [Example: Displaying Information About ICMP Rate-Limited Counters, page 84](#)
- [Example: Displaying IPv6 Interface Statistics, page 85](#)

Example: Customizing the Parameters for IPv6 Neighbor Discovery

In the following example, IPv6 ND NA gleaning is enabled and the IPv6 ND cache expiry is set to 7200 seconds (2 hours):

```
interface Port-channel189
no ip address
ipv6 address FC07::789:1:0:0:3/64
ipv6 nd reachable-time 2700000
ipv6 nd na glean
ipv6 nd cache expire 7200
no ipv6 redirects
standby version 2
standby 2 ipv6 FC07::789:1:0:0:1/64
standby 2 priority 150
standby 2 preempt
```

Example: IPv6 ICMP Rate Limiting Configuration

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
```

Example: Displaying Information About ICMP Rate-Limited Counters

In the following example, information about ICMP rate-limited counters is displayed:

```
Device# show ipv6 traffic
```

```
ICMP statistics:
  Rcvd: 188 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        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
        1 router solicit, 175 router advert, 0 redirects
        0 neighbor solicit, 12 neighbor advert
  Sent: 7376 output, 56 rate-limited
        unreach: 0 routing, 15 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout, 0 too big
        15 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 7326 router advert, 0 redirects
        2 neighbor solicit, 22 neighbor advert
```

Example: Displaying IPv6 Interface Statistics

In the following example, the **show ipv6 interface** command is used to verify that IPv6 addresses are configured correctly for FastEthernet interface 1/0. Information may also be displayed about the status of IPv6 neighbor redirect messages, IPv6 neighbor discovery messages, stateless autoconfiguration, and MTU size.

```
Device# show ipv6 interface fastethernet 1/0

Ethernet0 is up, line protocol is up
  IPv6 is stalled, link-local address is FE80::1
  Global unicast address(es):
    2001:DB8:2000::1, subnet is 2001:DB8:2000::/64
    2001:DB8:3000::1, subnet is 2001:DB8:3000::/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 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.
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Neighbor Discovery

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 15 *Feature Information for IPv6 Neighbor Discovery*

Feature Name	Releases	Feature Information
IPv6 Neighbor Discovery	12.0(22)S	The IPv6 neighbor discovery process uses ICMP messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and track neighboring devices.
	12.2(2)T	
	12.2(14)S	
	12.2(17a)SX1	
	12.2(25)SG	
	12.2(28)SB	
	12.2(33)SRA	The following commands were introduced or modified: ipv6 nd cache expire , ipv6 nd na glean , ipv6 nd nud retry .
	Cisco IOS XE Release 2.1 3.2.0SG	

Feature Name	Releases	Feature Information
IPv6: ICMPv6	12.0(22)S	ICMP in IPv6 functions the same as ICMP in IPv4. ICMP generates error messages, such as ICMP destination unreachable messages, and informational messages, such as ICMP echo request and reply messages. No commands were introduced or modified.
	12.2(2)T	
	12.2(14)S	
	12.2(17a)SX1	
	12.2(25)SG	
	12.2(28)SB	
	12.2(33)SRA	
	Cisco IOS XE Release 2.1	
IPv6: ICMPv6 Redirect	12.0(22)S	The IPv6 Redirect Messages feature enables a device to send ICMP IPv6 neighbor redirect messages to inform hosts of better first-hop nodes on the path to a destination. The following commands were introduced or modified: show ipv6 interface , show ipv6 neighbors , show ipv6 route , show ipv6 traffic .
	12.2(4)T	
	12.2(14)S	
	12.2(17a)SX1	
	12.2(25)SG	
	12.2(28)SB	
	12.2(33)SRA	
	Cisco IOS XE Release 2.1	
IPv6 ICMP Rate Limiting	12.2(8)T	The IPv6 ICMP Rate Limiting feature implements a token bucket algorithm for limiting the rate at which IPv6 ICMP error messages are sent out on the network. The following command was introduced or modified: ipv6 icmp error-interval .
	Cisco IOS XE Release 2.1	
IPv6: Neighbor Discovery Duplicate Address Detection	12.0(22)S	IPv6 neighbor discovery duplicate address detection is performed first on a new, link-local IPv6 address before the address is assigned to an interface (the new address remains in a tentative state while duplicate address detection is performed).
	12.2(4)T	
	12.2(17a)SX1	
	12.2(14)S	
	12.2(25)SG	
	12.2(28)SB	
	12.2(33)SRA	
	Cisco IOS XE Release 2.1	

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



IPv6 Neighbor Discovery Cache

The IPv6 neighbor discovery cache feature allows static entries to be made in the IPv6 neighbor cache.

The per-interface neighbor discovery cache limit function can be used to prevent any particular customer attached to an interface from overloading the neighbor discovery cache, whether intentionally or unintentionally.

- [Finding Feature Information, page 89](#)
- [Information About IPv6 Static Cache Entry for Neighbor Discovery, page 89](#)
- [How to Configure IPv6 Neighbor Discovery Cache, page 90](#)
- [Configuration Examples for IPv6 Neighbor Discovery Cache, page 92](#)
- [Additional References, page 92](#)
- [Feature Information for IPv6 Neighbor Discovery Cache, page 93](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPv6 Static Cache Entry for Neighbor Discovery

- [IPv6 Neighbor Discovery, page 89](#)
- [Per-Interface Neighbor Discovery Cache Limit, page 90](#)

IPv6 Neighbor Discovery

The IPv6 neighbor discovery process uses ICMP messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and track neighboring devices.

The IPv6 static cache entry for neighbor discovery feature allows static entries to be made in the IPv6 neighbor cache. Static routing requires an administrator to manually enter IPv6 addresses, subnet masks,

gateways, and corresponding Media Access Control (MAC) addresses for each interface of each device into a table. Static routing enables more control but requires more work to maintain the table. The table must be updated each time routes are added or changed.

Per-Interface Neighbor Discovery Cache Limit

The number of entries in the Neighbor Discovery cache can be limited by interface. Once the limit is reached, no new entries are allowed. The per-interface Neighbor Discovery cache limit function can be used to prevent any particular customer attached to an interface from overloading the Neighbor Discovery cache, whether intentionally or unintentionally.

When this feature is enabled globally, a common per-interface cache size limit is configured on all interfaces on the device. When this feature is enabled per interface, a cache size limit is configured on the associated interface. The per-interface limit overrides any globally configured limit.

How to Configure IPv6 Neighbor Discovery Cache

- [Configuring a Neighbor Discovery Cache Limit on a Specified Interface, page 90](#)
- [Configuring a Neighbor Discovery Cache Limit on All Device Interfaces, page 91](#)

Configuring a Neighbor Discovery Cache Limit on a Specified Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *type number***
4. **ipv6 nd cache interface-limit *size* [*log rate*]**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.

Command or Action	Purpose
Step 3 <code>interface type number</code> Example: <pre>Device(config)# interface GigabitEthernet 1/0/0</pre>	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4 <code>ipv6 nd cache interface-limit size [log rate]</code> Example: <pre>Device(config-if)# ipv6 nd cache interface- limit 1</pre>	Configures a Neighbor Discovery cache limit on a specified interface on the device. <ul style="list-style-type: none"> Issuing this command overrides any configuration that may have been created by issuing the ipv6 nd cache interface-limit in global configuration mode.

Configuring a Neighbor Discovery Cache Limit on All Device Interfaces

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ipv6 nd cache interface-limit size [log rate]`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3 <code>ipv6 nd cache interface-limit size [log rate]</code> Example: <pre>Device(config)# ipv6 nd cache interface-limit 4</pre>	Configures a neighbor discovery cache limit on all interfaces on the device.

Configuration Examples for IPv6 Neighbor Discovery Cache

- [Example: Configuring a Neighbor Discovery Cache Limit, page 92](#)

Example: Configuring a Neighbor Discovery Cache Limit

```
Device# show ipv6 interface GigabitEthernet2/0/0

Interface GigabitEthernet2/0/0, entries 2, static 0, limit 4

IPv6 Address          Age Link-layer Addr State  Interface
2001:0db8::94         0 aabb.cc00.5d02  REACH  GE2/0/0
FE80::A8BB:CCFF:FE00:5D02 0 aabb.cc00.5d02  DELAY  GE2/0/0
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Neighbor Discovery Cache

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 16 Feature Information for IPv6 Neighbor Discovery Cache

Feature Name	Releases	Feature Information
IPv6: Per-Interface Neighbor Discovery Cache Limit	15.1(3)T Cisco IOS XE Release 2.6	The per-interface neighbor discovery cache limit function can be used to prevent any particular customer attached to an interface from overloading the neighbor discovery cache, whether intentionally or unintentionally. The following commands were introduced or modified: ipv6 nd cache interface-limit , show ipv6 interface .

Feature Name	Releases	Feature Information
IPv6 Static Cache Entry for Neighbor Discovery	12.2(8)T	The IPv6 static cache entry for Neighbor Discovery feature allows static entries to be made in the IPv6 neighbor cache.
	12.2(17)SX1	
	12.2(25)SEA	The following commands were introduced or modified: ipv6 nd cache interface-limit , show ipv6 interface .
	12.2(25)SG	
	12.2(33)SRA	
	Cisco IOS XE Release 2.1	
	15.0(2)SG	
	3.2.0SG	

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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



IPv6 Stateless Autoconfiguration

The IPv6 stateless autoconfiguration feature can be used to manage link, subnet, and site addressing changes.

- [Finding Feature Information, page 95](#)
- [Information About IPv6 Stateless Autoconfiguration, page 95](#)
- [How to Configure IPv6 Stateless Autoconfiguration, page 96](#)
- [Configuration Examples for IPv6 Stateless Autoconfiguration, page 97](#)
- [Additional References, page 98](#)
- [Feature Information for IPv6 Stateless Autoconfiguration, page 99](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPv6 Stateless Autoconfiguration

- [IPv6 Stateless Autoconfiguration, page 95](#)
- [Simplified Network Renumbering for IPv6 Hosts, page 96](#)

IPv6 Stateless Autoconfiguration

All interfaces on IPv6 nodes must have a link-local address, which is usually automatically configured from the identifier for an interface and the link-local prefix FE80::/10. A link-local address enables a node to communicate with other nodes on the link and can be used to further configure the node.

Nodes can connect to a network and automatically generate global IPv6 addresses without the need for manual configuration or help of a server, such as a Dynamic Host Configuration Protocol (DHCP) server. With IPv6, a device on the link advertises any global prefixes in Router Advertisement (RA) messages, as well as its willingness to function as a default device for the link. RA messages are sent periodically and in response to device solicitation messages, which are sent by hosts at system startup.

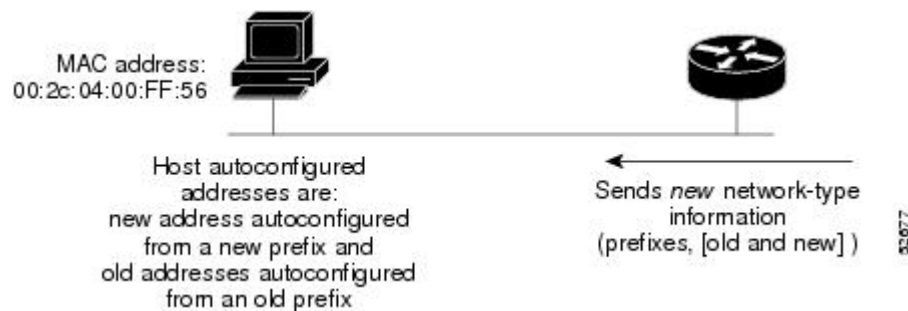
A node on the link can automatically configure global IPv6 addresses by appending its interface identifier (64 bits) to the prefixes (64 bits) included in the RA messages. The resulting 128-bit IPv6 addresses

configured by the node are then subjected to duplicate address detection to ensure their uniqueness on the link. If the prefixes advertised in the RA messages are globally unique, then the IPv6 addresses configured by the node are also guaranteed to be globally unique. Device solicitation messages, which have a value of 133 in the Type field of the ICMP packet header, are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled RA message.

Simplified Network Renumbering for IPv6 Hosts

The strict aggregation of the global routing table requires that networks be renumbered when the service provider for the network is changed. When the stateless autoconfiguration functionality in IPv6 is used to renumber a network, the prefix from a new service provider is added to RA messages that are sent on the link. (The RA messages contain both the prefix from the old service provider and the prefix from the new service provider.) Nodes on the link automatically configure additional addresses by using the prefix from the new service provider. The nodes can then use the addresses created from the new prefix and the existing addresses created from the old prefix on the link. Configuration of the lifetime parameters associated with the old and new prefixes means that nodes on the link can make the transition to using only addresses created from the new prefix. During a transition period, the old prefix is removed from RA messages and only addresses that contain the new prefix are used on the link (the renumbering is complete) (see the figure below).

Figure 19 IPv6 Network Renumbering for Hosts Using Stateless Autoconfiguration



How to Configure IPv6 Stateless Autoconfiguration

- [Enabling IPv6 Stateless Autoconfiguration, page 96](#)

Enabling IPv6 Stateless Autoconfiguration

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address autoconfig**

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: Device> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3 <code>interface type number</code> Example: Device(config)# <code>interface GigabitEthernet 0/0/0</code>	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4 <code>ipv6 address autoconfig</code> Example: Device(config-if)# <code>ipv6 address autoconfig</code>	Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6 processing on the interface.

Configuration Examples for IPv6 Stateless Autoconfiguration

- [Example: Displaying IPv6 Interface Statistics, page 97](#)

Example: Displaying IPv6 Interface Statistics

In the following example, the **show ipv6 interface** command is used to verify that IPv6 addresses are configured correctly for GigabitEthernet interface 0/0/0. Information is also displayed about the status of IPv6 neighbor redirect messages, IPv6 neighbor discovery messages, and stateless autoconfiguration.

```
Device# show ipv6 interface gigabitethernet 0/0/0

GigabitEthernet0/0/0 is up, line protocol is up
IPv6 is stalled, link-local address is FE80::1
Global unicast address(es):
  2001:DB8:2000::1, subnet is 2001:DB8:2000::/64
  2001:DB8:3000::1, subnet is 2001:DB8:3000::/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 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.

```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Stateless Autoconfiguration

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 17 Feature Information for IPv6 Stateless Autoconfiguration

Feature Name	Releases	Feature Information
IPv6 Stateless Autoconfiguration	12.2(2)T	The IPv6 stateless autoconfiguration feature can be used to manage link, subnet, and site addressing changes.
	12.2(17a)SX1	
	12.2(25)SEA	
	12.2(33)SRA	The following command was introduced or modified: ipv6 address autoconfig .
	12.2(25)SG	
	15.0(2)SG	
	Cisco IOS XE Release 2.1	
	3.2.0SG	

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams,

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.