Configuring IPv6 Unicast Routing

Information About IPv6 Unicast Routing

This chapter describes how to configure IPv6 host functions on the .

For information about configuring IPv6 Multicast Listener Discovery (MLD) snooping, see *Configuring MLD Snooping*.

Understanding IPv6

IPv4 users can move to IPv6 and receive services such as end-to-end security, quality of service (QoS), and globally unique addresses. The IPv6 address space reduces the need for private addresses and Network Address Translation (NAT) processing by border routers at network edges.

For information about how Cisco Systems implements IPv6, go to:
http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

IPv6 Addresses

The switch supports only IPv6 unicast addresses. It does not support site-local unicast addresses, or anycast addresses.

The IPv6 128-bit addresses are represented as a series of eight 16-bit hexadecimal fields separated by colons in the format: n:n:n:n:n:n:n:n. This is an example of an IPv6 address:

2031:0000:130F:0000:0000:09C0:080F:130B

For easier implementation, leading zeros in each field are optional. This is the same address without leading zeros:

2031:0:130F:0:0:9C0:80F:130B

You can also use two colons (::) to represent successive hexadecimal fields of zeros, but you can use this short version only once in each address:

2031:0:130F::09C0:080F:130B

For more information about IPv6 address formats, address types, and the IPv6 packet header, see the http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-3e/ip6b-xe-3e-book.html of *Cisco IOS IPv6 Configuration Library* on Cisco.com.

Supported IPv6 Unicast Routing Features

The following sections describe the IPv6 protocol features supported by the switch:

128-Bit Wide Unicast Addresses

The switch supports aggregatable global unicast addresses and link-local unicast addresses. It does not support site-local unicast addresses.

- Aggregatable global unicast addresses are IPv6 addresses from the aggregatable global unicast prefix. The address structure enables strict aggregation of routing prefixes and limits the number of routing table entries in the global routing table. These addresses are used on links that are aggregated through organizations and eventually to the Internet service provider.

  These addresses are defined by a global routing prefix, a subnet ID, and an interface ID. Current global unicast address allocation uses the range of addresses that start with binary value 001 (2000::/3). Addresses with a prefix of 2000::/3(001) through E000::/3(111) must have 64-bit interface identifiers in the extended unique identifier (EUI)-64 format.

- Link local unicast addresses can be automatically configured on any interface by using the link-local prefix FE80::/10(1111 1110 10) and the interface identifier in the modified EUI format. Link-local addresses are used in the neighbor discovery protocol (NDP) and the stateless autoconfiguration process. Nodes on a local link use link-local addresses and do not require globally unique addresses to communicate. IPv6 routers do not forward packets with link-local source or destination addresses to other links.

DNS for IPv6

IPv6 supports Domain Name System (DNS) record types in the DNS name-to-address and address-to-name lookup processes. The DNS AAAA resource record types support IPv6 addresses and are equivalent to an A address record in IPv4. The switch supports DNS resolution for IPv4 and IPv6.

ICMPv6

The Internet Control Message Protocol (ICMP) in IPv6 generates error messages, such as ICMP destination unreachable messages, to report errors during processing and other diagnostic functions. In IPv6, ICMP packets are also used in the neighbor discovery protocol and path MTU discovery.

Neighbor Discovery

The switch supports Neighbor Discovery Protocol (NDP) for IPv6, a protocol running on top of ICMPv6, and static neighbor entries for IPv6 stations that do not support NDP. 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), to verify the reachability of the neighbor, and to keep track of neighboring routers.

The switch supports ICMPv6 redirect for routes with mask lengths less than 64 bits. ICMP redirect is not supported for host routes or for summarized routes with mask lengths greater than 64 bits.

Neighbor discovery throttling ensures that the switch CPU is not unnecessarily burdened while it is in the process of obtaining the next hop forwarding information to route an IPv6 packet. The switch drops any

additional IPv6 packets whose next hop is the same neighbor that the switch is actively trying to resolve. This drop avoids further load on the CPU.

Note   IPv6 next hop security features are not supported in .

IPv6 Stateless Autoconfiguration and Duplicate Address Detection

The switch uses stateless autoconfiguration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses. A host autonomously configures its own link-local address, and booting nodes send router solicitations to request router advertisements for configuring interfaces.

IPv6 Applications

The switch has IPv6 support for these applications:

- Ping, traceroute, Telnet

- Secure Shell (SSH) over an IPv6 transport

- HTTP server access over IPv6 transport

- DNS resolver for AAAA over IPv4 transport

- Cisco Discovery Protocol (CDP) support for IPv6 addresses

Static Routes for IPv6

Static routes are manually configured and define an explicit route between two networking devices. Static routes are useful for smaller networks with only one path to an outside network or to provide security for certain types of traffic in a larger network.

RIP for IPv6

Routing Information Protocol (RIP) for IPv6 is a distance-vector protocol that uses hop count as a routing metric. It includes support for IPv6 addresses and prefixes and the all-RIP-routers multicast group address FF02::9 as the destination address for RIP update messages.

SNMP and Syslog Over IPv6

To support both IPv4 and IPv6, IPv6 network management requires both IPv6 and IPv4 transports. Syslog over IPv6 supports address data types for these transports.

Simple Network Management Protocol (SNMP) and syslog over IPv6 provide these features:

- Support for both IPv4 and IPv6

- IPv6 transport for SNMP and to modify the SNMP agent to support traps for an IPv6 host

- SNMP- and syslog-related MIBs to support IPv6 addressing

- Configuration of IPv6 hosts as trap receivers

For support over IPv6, SNMP modifies the existing IP transport mapping to simultaneously support IPv4 and IPv6. These SNMP actions support IPv6 transport management:

- Opens User Datagram Protocol (UDP) SNMP socket with default settings

• Provides a new transport mechanism called *SR_IPV6_TRANSPORT*

• Sends SNMP notifications over IPv6 transport

• Supports SNMP-named access lists for IPv6 transport

• Supports SNMP proxy forwarding using IPv6 transport

• Verifies SNMP Manager feature works with IPv6 transport

HTTP(S) Over IPv6

The HTTP client sends requests to both IPv4 and IPv6 HTTP servers, which respond to requests from both IPv4 and IPv6 HTTP clients. URLs with literal IPv6 addresses must be specified in hexadecimal using 16-bit values between colons.

The accept socket call chooses an IPv4 or IPv6 address family. The accept socket is either an IPv4 or IPv6 socket. The listening socket continues to listen for both IPv4 and IPv6 signals that indicate a connection. The IPv6 listening socket is bound to an IPv6 wildcard address.

The underlying TCP/IP stack supports a dual-stack environment. HTTP relies on the TCP/IP stack and the sockets for processing network-layer interactions.

Basic network connectivity (**ping**) must exist between the client and the server hosts before HTTP connections can be made.

Default IPv6 Configuration

Table 1: Default IPv6 Configuration

Feature	Default Setting
IPv6 addresses	None configured

How to Configure IPv6 Unicast Routing

Configuring IPv6 Addressing and Enabling IPv6 Routing

This section describes how to assign IPv6 addresses to individual Layer 3 interfaces and to globally forward IPv6 traffic on the switch.

Before configuring IPv6 on the switch, note the following:

In the **ipv6 address** interface configuration command, you must enter the *ipv6-address* and *ipv6-prefix* variables with the address specified in hexadecimal using 16-bit values between colons. The *prefix-length* variable (preceded by a slash [/]) is a decimal value that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

To forward IPv6 traffic on an interface, you must configure a global IPv6 address on that interface. Configuring an IPv6 address on an interface automatically configures a link-local address and activates IPv6 for the interface. The configured interface automatically joins these required multicast groups for that link:

- solicited-node multicast group FF02:0:0:0:0:1:ff00::/104 for each unicast address assigned to the interface (this address is used in the neighbor discovery process.)

- all-nodes link-local multicast group FF02::1

- all-routers link-local multicast group FF02::2

Beginning in privileged EXEC mode, follow these steps to assign an IPv6 address to a Layer 3 interface and enable IPv6 forwarding:

Procedure

	Command or Action	**Purpose**
Step 1	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** Device(config)# **interface gigabitethernet 1/0/1** Or Device(config)# **interface fastethernet 1/0/1**	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
Step 3	Use one of the following: 　• **ipv6 address** *ipv6-prefix/prefix length* **eui-64** 　• **ipv6 address** *ipv6-address/prefix length* 　• **ipv6 address** *ipv6-address* **link-local** 　• **ipv6 enable** **Example:** Device(config-if)# **ipv6 address 2001:0DB8:c18:1::/64 eui 64** Device(config-if)# **ipv6 address 2001:0DB8:c18:1::/64** Device(config-if)# **ipv6 address FE80::/10 link-local** Device(config-if)# **ipv6 enable**	• **ipv6 address** *ipv6-prefix/prefix length* **eui-64**: Specifies a global IPv6 address with an extended unique identifier (EUI) in the low-order 64 bits of the IPv6 address. Specify only the network prefix; the last 64 bits are automatically computed from the switch MAC address. This enables IPv6 processing on the interface. • **ipv6 address** *ipv6-address/prefix length*: Manually configures an IPv6 address on the interface. • **ipv6 address** *ipv6-address* **link-local**: Specifies a link-local address to be used on the interface instead of the link-local address that is automatically configured when IPv6 is enabled on the interface. This command enables IPv6 processing on the interface. • **ipv6 enable**: Automatically configures an IPv6 link-local address on the interface, and enables the interface for IPv6 processing. The link-local address can only

	Command or Action	Purpose
		be used to communicate with nodes on the same link.
Step 4	**end** **Example:** Device(config-if)#**end**	Returns to privileged EXEC mode.
Step 5	**show ipv6 interface** *interface-id* **Example:** Device# **show ipv6 interface gigabitethernet 1/0/1** Or Device# **show ipv6 interface fastethernet 1/0/1**	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** Device# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Configuring IPv6 ICMP Rate Limiting

ICMP rate limiting is enabled by default with a default interval between error messages of 100 milliseconds and a bucket size (maximum number of tokens to be stored in a bucket) of 10.

Beginning in privileged EXEC mode, follow these steps to change the ICMP rate-limiting parameters:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.
Step 2	**ipv6 icmp error-interval** *interval* [*bucketsize*] **Example:** Device(config)# **ipv6 icmp error-interval 50 20**	Configures the interval and bucket size for IPv6 ICMP error messages: • *interval*—The interval (in milliseconds) between tokens being added to the bucket. The range is from 0 to 2147483647 milliseconds.

	Command or Action	Purpose
		• *bucketsize*—(Optional) The maximum number of tokens stored in the bucket. The range is from 1 to 200.
Step 3	**end**	Returns to privileged EXEC mode.
	Example:	
	Device(config)# **end**	
Step 4	**show ipv6 interface** [*interface-id*]	Verifies your entries.
	Example:	
	Device# **show ipv6 interface gigabitethernet 1/0/1**	
	Or	
	Device# **show ipv6 interface fastethernet 1/0/1**	
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.
	Example:	
	Device# **copy running-config startup-config**	

Configuring Static Routing for IPv6 (CLI)

Beginning in privileged EXEC mode, follow these steps to configure a static IPv6 route:

Note The switch supports 16 IPv6 static routes.

Before you begin

Before configuring a static IPv6 route, you must:

- Enable routing by using the **ip routing** global configuration command.
- Enable the forwarding of IPv6 packets by using the **ipv6 unicast-routing** global configuration command.
- Enable IPv6 on at least one Layer 3 interface by configuring an IPv6 address on the interface.

Procedure

	Command or Action	**Purpose**
Step 1	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.
Step 2	**ipv6 route** *ipv6-prefix/prefix length* {*ipv6-address* | *interface-id* [*ipv6-address*]} [*administrative distance*] **Example:** Device(config)# **ipv6 route 2001:0DB8::/32 gigabitethernet 1/0/1 130** Or Device(config)# **ipv6 route 2001:0DB8::/32 fastethernet 0/1 130**	Configures a static IPv6 route. You must configure one of the following options: • *ipv6-prefix*: The IPv6 network that is the destination of the static route. It can also be a hostname when static host routes are configured. • */prefix length*: The length of the IPv6 prefix. A decimal value that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. • *ipv6-address*: The IPv6 address of the next hop that can be used to reach the specified network. The IPv6 address of the next hop need not be directly connected; recursion is done to find the IPv6 address of the directly connected next hop. The address must be in the form documented in RFC 2373, specified in hexadecimal using 16-bit values between colons. • *interface-id*: Specifies direct static routes from point-to-point and broadcast interfaces. With point-to-point interfaces, there is no need to specify the IPv6 address of the next hop. With broadcast interfaces, you should always specify the IPv6 address of the next hop, or ensure that the specified prefix is assigned to the link, specifying a link-local address as the next hop. You can optionally specify the IPv6 address of the next hop to which packets are sent. **Note** You must specify an *interface-id* when using a link-local address as the next hop (the link-local next hop must also be an adjacent router).

		Command or Action	Purpose
			• *administrative distance*—(Optional) An administrative distance. The range is 1 to 254; the default value is 1, which gives static routes precedence over any other type of route except connected routes. To configure a floating static route, use an administrative distance greater than that of the dynamic routing protocol.
Step 3		**end** **Example:** Device(config)# **end**	Returns to privileged EXEC mode.

Step 4		Use one of the following:
		
		• **show ipv6 static** [*ipv6-address* | *ipv6-prefix/prefix length*] [**interface** *interface-id*] [**detail**]][**recursive**] [**detail**]
		• **show ipv6 route static**
		
		Example:
		
		Device# **show ipv6 static 2001:0DB8::/32 interface gigabitethernet 1/0/1**
		
		or
		
		Device# **show ipv6 route static**
			Verifies your entries by displaying the contents of the IPv6 routing table.
			
			• **interface** *interface-id* (Optional): Displays only those static routes with the specified interface as an egress interface.
			
			• **recursive**(Optional): Displays only recursive static routes. The **recursive** keyword is mutually exclusive with the **interface** keyword, but it can be used with or without the IPv6 prefix included in the command syntax.
			
			• **detail**(Optional): Displays this additional information:
			
			    • For valid recursive routes, the output path set, and maximum resolution depth.
			
			    • For invalid routes, the reason why the route is not valid.

Step 5		**copy running-config startup-config** **Example:** Device# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Configuring RIP for IPv6

Beginning in privileged EXEC mode, follow these steps to configure RIP routing for IPv6:

Before you begin

Before configuring the switch to run IPv6 RIP, you must:

- Enable routing by using the **ip routing** global configuration command.

- Enable the forwarding of IPv6 packets by using the **ipv6 unicast-routing** global configuration command.

- Enable IPv6 on at least one Layer 3 interface by configuring an IPv6 address on the interface.

Procedure

	Command or Action	**Purpose**
Step 1	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.
Step 2	**ipv6 router rip** *name* **Example:** Device(config)# **ipv6 router rip cisco**	Configures an IPv6 RIP routing process, and enters router configuration mode for the process.
Step 3	**maximum-paths** *number-paths* **Example:** Device(config-router)# **maximum-paths 6**	(Optional) Defines the maximum number of equal-cost routes that IPv6 RIP can support. The range is from 1 to 8, and the default is 8 routes.
Step 4	**exit** **Example:** Device(config-router)# **exit**	Returns to global configuration mode.
Step 5	**interface** *interface-id* **Example:** Device(config)# **interface gigabitethernet 1/0/1** Or Device(config)# **interface fastethernet 1/0/1**	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
Step 6	**ipv6 rip** *name* **enable** **Example:** Device(config-if)# **ipv6 rip cisco enable**	Enables the specified IPv6 RIP routing process on the interface.
Step 7	**ipv6 rip** *name* **default-information** {**only** | **originate**} **Example:**	(Optional) Originates the IPv6 default route (::/0) into the RIP routing process updates sent from the specified interface.

	Command or Action	Purpose
	Device(config-if)# **ipv6 rip cisco default-information only**	**Note** To avoid routing loops after the IPv6 default route (::/0) is originated from any interface, the routing process ignores all default routes received on any interface. • **only**: Select to originate the default route, but suppress all other routes in the updates sent on this interface. • **originate**: Select to originate the default route in addition to all other routes in the updates sent on this interface.
Step 8	**end** **Example:** Device(config)# **end**	Returns to privileged EXEC mode.
Step 9	Use one of the following: • **show ipv6 rip** [*name*] [**interface** *interface-id*] [**database**] [**next-hops**] • **show ipv6 rip** **Example:** Device# **show ipv6 rip cisco interface gigabitethernet 1/0/1** or Device# **show ipv6 rip**	• The **show ipv6 rip cisco interface** command displays information about current IPv6 RIP processes. • The **show ipv6 rip** command displays the current contents of the IPv6 routing table.
Step 10	**copy running-config startup-config** **Example:** Device# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Monitoring IPv6 Unicast Routing

Displaying IPv6

The following table lists the commands you can use to monitor IPv6 unicast routing features. For complete syntax and usage information for these commands, see the command reference document.

Command	Purpose
show ipv6 access-list	Displays a summary of access lists.
show ipv6 cef	Displays Cisco Express Forwarding for IPv6.
show ipv6 interface *interface-id*	Displays IPv6 interface status and configuration.
show ipv6 neighbors	Displays IPv6 neighbor cache entries.
show ipv6 prefix-list	Displays a list of IPv6 prefix lists.
show ipv6 protocols	Displays a list of IPv6 routing protocols on the switch.
show ipv6 rip	Displays IPv6 RIP routing protocol status.
show ipv6 route	Displays IPv6 route table entries.
show ipv6 static	Displays IPv6 static routes.
show ipv6 traffic	Displays IPv6 traffic statistics.

Configuration Examples for IPv6 Unicast Routing

Example: Configuring IPv6 Addressing and Enabling IPv6 Routing

This example shows how to enable IPv6 with both a link-local address and a global address based on the IPv6 prefix 2001:0DB8: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** EXEC command is included to show how the interface ID (20B:46FF:FE2F:D940) is appended to the link-local prefix FE80::/64 of the interface.

```
Device(config)# ipv6 unicast-routing
Device(config)# interface gigabitethernet 1/0/11
Device(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Device(config-if)# end
Device# show ipv6 interface gigabitethernet 1/0/11
GigabitEthernet1/0/11 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
  2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  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.
```

Example: Configuring IPv6 ICMP Rate Limiting

This example shows how to configure an IPv6 ICMP error message interval of 50 milliseconds and a bucket size of 20 tokens.

```
Device(config)#ipv6 icmp error-interval 50 20
```

Example: Configuring Static Routing for IPv6

This example shows how to configure a floating static route to an interface with an administrative distance of 130:

```
Device(config)# ipv6 route 2001:0DB8::/32 gigabitethernet 1/0/1 130
```

Example: Displaying IPv6

This is an example of the output from the **show ipv6 interface** privileged EXEC command:

```
De# show ipv6 interface
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
    3FFE:C000:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:C000:0:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  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
<output truncated>
```

Feature History and Information for IPv6 Unicast Routing

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 the 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.

Feature Name	Release	Modification
IPv6 Unicast Routing	Cisco IOS Release 15.2(7)E1	This feature was introduced.