



# CHAPTER 40

## Configuring IPv6 Unicast Routing

Internet Protocol Version 6 (IPv6) is the network-layer Internet Protocol intended to replace Version 4 (IPv4) in the TCP/IP suite of protocols. This chapter describes how to configure IPv6 unicast routing on the switch.

For information about configuring IPv4 unicast routing, see [Chapter 39, “Configuring IP Unicast Routing.”](#) For information about configuring IPv6 Multicast Listener Discovery (MLD) snooping, see [Chapter 25, “Configuring IPv6 MLD Snooping.”](#) For information on configuring IPv6 access control lists (ACLs) see [Chapter 36, “Configuring IPv6 ACLs.”](#)

To use this feature, the switch or stack master must be running the IP services feature set. This feature set includes all IP services features plus IPv6 host and unicast routing support.

To enable IPv6 routing, you must configure the switch to use the a dual IPv4 and IPv6 switch database management (SDM) template. See the [“Dual IPv4 and IPv6 Protocol Stacks” section on page 40-6.](#)

Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.



### Note

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS documentation referenced in the procedures

This chapter consists of these sections:

- [“Understanding IPv6” section on page 40-1](#)
- [“Configuring IPv6” section on page 40-12](#)
- [“Displaying IPv6” section on page 40-29](#)

## 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 this URL:

[http://www.cisco.com/en/US/products/ps6553/products\\_ios\\_technology\\_home.html](http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html)

For information about IPv6 and other features in this chapter

- See the *Cisco IOS IPv6 Configuration Library* at this URL:  
[http://www.cisco.com/en/US/docs/ios/12\\_2t/ipv6/ipv6\\_vgf.html](http://www.cisco.com/en/US/docs/ios/12_2t/ipv6/ipv6_vgf.html)

- Use the Search field to locate the Cisco IOS software documentation. For example, if you want information about static routes, you can enter *Implementing Static Routes for IPv6* in the search field to get this document about static routes:

[http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-stat\\_routes\\_ps6441\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-stat_routes_ps6441_TSD_Products_Configuration_Guide_Chapter.html)

This section describes IPv6 implementation on the switch. These sections are included:

- [IPv6 Addresses, page 40-2](#)
- [Supported IPv6 Unicast Routing Features, page 40-3](#)
- [Unsupported IPv6 and Unicast Routing Features, page 40-9](#)
- [Limitations, page 40-9](#)
- [IPv6 and Switch Stacks, page 40-10](#)

## IPv6 Addresses

The switch supports only IPv6 unicast addresses. It does not support site-local unicast addresses, anycast addresses, or multicast 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 “Implementing IPv6 Addressing and Basic Connectivity” chapter of *Cisco IOS IPv6 Configuration Library* on Cisco.com.

In the “Information About Implementing Basic Connectivity for IPv6” chapter, these sections apply to the switch:

- IPv6 Address Formats
- IPv6 Address Type: Unicast
- IPv6 Address Output Display
- Simplified IPv6 Packet Header

## Supported IPv6 Unicast Routing Features

These sections describe the IPv6 protocol features supported by the switch:

- [128-Bit Wide Unicast Addresses, page 40-4](#)
- [DNS for IPv6, page 40-4](#)
- [Path MTU Discovery for IPv6 Unicast, page 40-4](#)
- [ICMPv6, page 40-4](#)
- [Neighbor Discovery, page 40-4](#)
- [Default Router Preference, page 40-5](#)
- [IPv6 Stateless Autoconfiguration and Duplicate Address Detection, page 40-5](#)
- [IPv6 Applications, page 40-5](#)
- [Dual IPv4 and IPv6 Protocol Stacks, page 40-6](#)
- [DHCP for IPv6 Address Assignment, page 40-6](#)
- [Static Routes for IPv6, page 40-7](#)
- [RIP for IPv6, page 40-7](#)
- [OSPF for IPv6, page 40-7](#)
- [Authentication Support with IPsec, page 40-7](#)
- [EIGRP for IPv6, page 40-8](#)
- [HSRP for IPv6, page 40-8](#)
- [SNMP and Syslog Over IPv6, page 40-8](#)
- [HTTP\(S\) Over IPv6, page 40-9](#)

Support on the switch includes expanded address capability, header format simplification, improved support of extensions and options, and hardware parsing of the extension header. The switch supports hop-by-hop extension header packets, which are routed or bridged in software.

The switch provides IPv6 routing capability over 802.1Q trunk ports for static routes, Routing Information Protocol (RIP) for IPv6, and Open Shortest Path First (OSPF) Version 3 protocol. It supports up to 16 equal-cost routes and can forward IPv4 and IPv6 frames simultaneously at line rate.

## 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 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.

For more information, see the section about IPv6 unicast addresses in the “Implementing IPv6 Addressing and Basic Connectivity” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## 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.

## Path MTU Discovery for IPv6 Unicast

The switch supports advertising the system MTU to IPv6 nodes and path MTU discovery. Path MTU discovery allows a host to dynamically discover and adjust to differences in the MTU size of every link along a given data path. In IPv6, if a link along the path is not large enough to accommodate the packet size, the source of the packet handles the fragmentation. The switch does not support path MTU discovery for multicast packets.

## 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 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.

## Default Router Preference

The switch supports IPv6 default router preference (DRP), an extension in router advertisement messages. DRP improves the ability of a host to select an appropriate router, especially when the host is multihomed and the routers are on different links. The switch does not support the Route Information Option in RFC 4191.

An IPv6 host maintains a default router list from which it selects a router for traffic to offlink destinations. The selected router for a destination is then cached in the destination cache. NDP for IPv6 specifies that routers that are reachable or probably reachable are preferred over routers whose reachability is unknown or suspect. For reachable or probably reachable routers, NDP can either select the same router every time or cycle through the router list. By using DRP, you can configure an IPv6 host to prefer one router over another, provided both are reachable or probably reachable.

For more information about DRP for IPv6, see the “Implementing IPv6 Addresses and Basic Connectivity” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## 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.

For more information about autoconfiguration and duplicate address detection, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter of *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## IPv6 Applications

The switch has IPv6 support for these applications:

- Ping, traceroute, Telnet, and TFTP
- 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

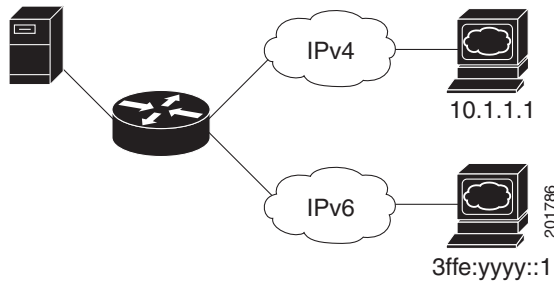
For more information about managing these applications, see the “Managing Cisco IOS Applications over IPv6” chapter and the “Implementing IPv6 Addressing and Basic Connectivity” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## Dual IPv4 and IPv6 Protocol Stacks

You must use the dual IPv4 and IPv6 template to allocate ternary content addressable memory (TCAM) usage to both IPv4 and IPv6 protocols.

Figure 40-1 shows a router forwarding both IPv4 and IPv6 traffic through the same interface, based on the IP packet and destination addresses.

**Figure 40-1 Dual IPv4 and IPv6 Support on an Interface**



Use the dual IPv4 and IPv6 switch database management (SDM) template to enable IPv6 routing. For more information about the dual IPv4 and IPv6 SDM template, see [Chapter 8, “Configuring SDM Templates.”](#)

The dual IPv4 and IPv6 templates allow the switch to be used in dual stack environments.

- If you try to configure IPv6 without first selecting a dual IPv4 and IPv6 template, a warning message appears.
- In IPv4-only environments, the switch routes IPv4 packets and applies IPv4 QoS and ACLs in hardware. IPv6 packets are not supported.
- In dual IPv4 and IPv6 environments, the switch routes both IPv4 and IPv6 packets and applies IPv4 QoS in hardware.
- The switch does not support IPv6 QoS.
- If you do not plan to use IPv6, do not use the dual stack template because this template results in less TCAM capacity for each resource.

For more information about IPv4 and IPv6 protocol stacks, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter of *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## DHCP for IPv6 Address Assignment

DHCPv6 enables DHCP servers to pass configuration parameters, such as IPv6 network addresses, to IPv6 clients. The address assignment feature manages nonduplicate address assignment in the correct prefix based on the network where the host is connected. Assigned addresses can be from one or multiple prefix pools. Additional options, such as default domain and DNS name-server address, can be passed back to the client. Address pools can be assigned for use on a specific interface, on multiple interfaces, or the server can automatically find the appropriate pool.

This document describes only the DHCPv6 address assignment. For more information about configuring the DHCPv6 client, server, or relay agent functions, see the “Implementing DHCP for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## 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.

For more information about static routes, see the “Implementing Static Routes for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## 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.

For more information about RIP for IPv6, see the “Implementing RIP for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## OSPF for IPv6

The switch supports Open Shortest Path First (OSPF) for IPv6, a link-state protocol for IP. For more information, see the “Implementing OSFP for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

Beginning with Cisco IOS Release 12.2(58)SE, switches running the IP-services feature set support the graceful restart feature in OSPFv3. This feature allows nonstop data forwarding along known routes while the OSPFv3 routing protocol information is being restored. A switch can participate in graceful restart either in restart mode (such as in a graceful-restart-capable switch) or in helper mode (such as in a graceful-restart-aware switch).

To perform the graceful restart function, a switch must be in high availability (HA) stateful switchover (SSO) mode (that is, dual RP). A switch capable of graceful restart performs the graceful restart function when these failures occur:

- A Route Processor (RP) failure that results in switchover to standby RP
- A planned RP switchover to standby RP

The graceful restart feature requires that neighboring switches be graceful-restart aware.

For more information, see the “Implementing OSFP for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## Authentication Support with IPsec

To ensure that OSPF for IPv6 (OSPFv3) packets are not altered and resent to the switch, OSPFv3 packets must be authenticated. OSPFv3 uses the IPsec secure socket API to add authentication to OSPFv3 packets. This API has been extended to provide support for IPv6.

OSPFv3 requires the use of IPsec to enable authentication. Crypto images are required to use authentication, because only crypto images include the IPsec API needed for use with OSPFv3.

For more information, see the [OSPFv3 Authentication Support with IPsec](#) section of the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## EIGRP for IPv6

The switch supports Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6. It is configured on the interfaces on which it runs and does not require a global IPv6 address.

Before running, an instance of EIGRP IPv6 requires an implicit or explicit router ID. An implicit router ID is derived from a local IPv4 address, so any IPv4 node always has an available router ID. However, EIGRP IPv6 might be running in a network with only IPv6 nodes and therefore might not have an available IPv4 router ID.

For more information about EIGRP for IPv6, see the “Implementing EIGRP for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## HSRP for IPv6

The switch supports the Hot Standby Router Protocol (HSRP) for IPv6. HSRP provides routing redundancy for routing IPv6 traffic not dependent on the availability of any single router. IPv6 hosts learn of available routers through IPv6 neighbor discovery router advertisement messages. These messages are multicast periodically or are solicited by hosts.

An HSRP IPv6 group has a virtual MAC address that is derived from the HSRP group number and a virtual IPv6 link-local address that is, by default, derived from the HSRP virtual MAC address. Periodic messages are sent for the HSRP virtual IPv6 link-local address when the HSRP group is active. These messages stop after a final one is sent when the group leaves the active state.

For more information about configuring HSRP for IPv6, see the “Configuring First Hop Redundancy Protocols in IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## 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.

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

For information on SNMP over IPv6, including configuration procedures, see the “Managing Cisco IOS Applications over IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.



For information about syslog over IPv6, including configuration procedures, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## 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.

For more information, see the “Managing Cisco IOS Applications over IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## Unsupported IPv6 and Unicast Routing Features

The switch does not support these IPv6 features:

- IPv6 policy-based routing
- IPv6 virtual private network (VPN) routing and forwarding (VRF) table support
- Support for IPv6 routing protocols: multiprotocol Border Gateway Protocol (BGP) and Intermediate System-to-Intermediate System (IS-IS) routing
- IPv6 packets destined to site-local addresses
- Tunneling protocols, such as IPv4-to-IPv6 or IPv6-to-IPv4
- The switch as a tunnel endpoint supporting IPv4-to-IPv6 or IPv6-to-IPv4 tunneling protocols
- IPv6 unicast reverse-path forwarding
- IPv6 general prefixes

## Limitations

Because IPv6 is implemented in switch hardware, some limitations occur due to the IPv6 compressed addresses in the hardware memory. These hardware limitations result in some loss of functionality and limits some features.

These are feature limitations.

- ICMPv6 redirect functionality is not supported for IPv6 host routes (routes used to reach a specific host) or for IPv6 routes with masks greater than 64 bits. The switch cannot redirect hosts to a better first-hop router for a specific destination that is reachable through a host route or through a route with masks greater than 64 bits.
- Load-balancing using equal cost and unequal cost routes is not supported for IPv6 host routes or for IPv6 routes with a mask greater than 64 bits.

- The switch cannot forward SNAP-encapsulated IPv6 packets.




---

**Note** There is a similar limitation for IPv4 SNAP-encapsulated packets, but the packets are dropped at the switch and are not forwarded.

---

- The switch routes IPv6-to-IPv4 and IPv4-to-IPv6 packets in hardware, but the switch cannot be an IPv6-to-IPv4 or IPv4-to-IPv6 tunnel endpoint.
- Bridged IPv6 packets with hop-by-hop extension headers are forwarded in software. In IPv4, these packets are routed in software, but bridged in hardware.
- In addition to the normal SPAN and RSPAN limitations defined in the software configuration guide, these limitations are specific to IPv6 packets:
  - When you send RSPAN IPv6-routed packets, the source MAC address in the SPAN output packet can be incorrect.
  - When you send RSPAN IPv6-routed packets, the destination MAC address can be incorrect. Normal traffic is not affected.
- The switch cannot apply QoS classification or policy-based routing on source-routed IPv6 packets in hardware.
- The switch cannot generate ICMPv6 *Packet Too Big* messages for multicast packets.

## IPv6 and Switch Stacks

The switch supports IPv6 forwarding across the stack and IPv6 host functionality on the stack master. The stack master runs the IPv6 unicast routing protocols and computes the routing tables. Using distributed CEF (dCEF), the stack master downloads the routing table to the stack member switches. They receive the tables and create hardware IPv6 routes for forwarding. The stack master also runs all IPv6 applications.




---

**Note** To route IPv6 packets in a stack, all switches in the stack must be running the IP services feature set.

---

If a new switch becomes the stack master, it recomputes the IPv6 routing tables and distributes them to the member switches. While the new stack master is being elected and is resetting, the switch stack does not forward IPv6 packets. The stack MAC address changes, which also changes the IPv6 address. When you specify the stack IPv6 address with an extended unique identifier (EUI) by using the **ipv6 address ipv6-prefix/prefix length eui-64** interface configuration command, the address is based on the interface MAC address. See the [“Configuring IPv6 Addressing and Enabling IPv6 Host Functions or Routing” section on page 40-13](#).

If you configure the persistent MAC address feature on the stack and the stack master changes, the stack MAC address does not change for approximately 4 minutes. For more information, see the [“Enabling Persistent MAC Address” section on page 7-22 in Chapter 7, “Managing Switch Stacks.”](#)

These are the functions of IPv6 stack master and members:

- Stack master:
  - runs IPv6 routing protocols
  - generates routing tables
  - distributes CEFv6 routing tables to stack members that use dCEFv6

- runs IPv6 host functionality and IPv6 applications

- Stack member (must be running the IP services feature set):
  - receives CEFv6 routing tables from the stack master
  - programs the routes into hardware



---

**Note** IPv6 packets are routed in hardware across the stack if the packet does not have exceptions (IPv6Options) and the switches in the stack have not run out of hardware resources.

---

- flushes the CEFv6 tables on master re-election

With IPv4 unicast routing, if the stack detects that the stack master is down and elects one of the stack members the new stack master, except for a momentary interruption, the hardware continues to forward packets with no active protocols. With IPv6, the switch does not continue forwarding packets. On election of a new stack master, the stack might need up to 60 seconds to recover all routes and resume forwarding traffic.

IPv6 host functionality is supported on the stack master, and all IPv6 applications run on the stack master.

## Configuring IPv6

These sections contain this IPv6 forwarding configuration information:

- [Default IPv6 Configuration, page 40-13](#)
- [Configuring IPv6 Addressing and Enabling IPv6 Host Functions or Routing, page 40-13](#)
- [Configuring Default Router Preference, page 40-15](#)
- [Configuring IPv4 and IPv6 Protocol Stacks, page 40-16](#)
- [Configuring DHCP for IPv6 Address Assignment, page 40-17](#)
- [Configuring IPv6 ICMP Rate Limiting, page 40-21](#)
- [Configuring CEF and dCEF for IPv6, page 40-21](#)
- [Configuring Static Routes for IPv6, page 40-22](#)
- [Configuring RIP for IPv6, page 40-23](#)
- [Configuring OSPF for IPv6, page 40-24](#)[Configuring IPsec on OSPFv3, page 40-26](#)
- [Configuring EIGRP for IPv6, page 40-26](#)
- [Configuring HSRP for IPv6, page 40-26](#)

## Default IPv6 Configuration

Table 40-1 shows the default IPv6 configuration.

**Table 40-1** Default IPv6 Configuration

Feature	Default Setting
SDM template	Default desktop.
IPv6 routing <sup>1</sup>	Disabled globally and on all interfaces.
CEFv6 or dCEFv6 <sup>1</sup>	Disabled (IPv4 CEF and dCEF are enabled by default).  <b>Note</b> When IPv6 routing is enabled, CEFv6 and dCEFv6 are automatically enabled.
IPv6 addresses	None configured.

1. This feature is supported only on the Catalyst Switch Module 3110.

## Configuring IPv6 Addressing and Enabling IPv6 Host Functions or 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, consider these guidelines:

- Be sure to select a dual IPv4 and IPv6 SDM template.
- Not all features discussed in this chapter are supported by the switch. See the “[Unsupported IPv6 and Unicast Routing Features](#)” section on page 40-9.
- 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 FF02:0:0:0:1: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

For more information about configuring IPv6 host functions or routing, see the “Implementing Addressing and Basic Connectivity for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

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

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>sdm prefer dual-ipv4-and-ipv6 { default   routing   vlan }</code>	Select an SDM template that supports IPv4 and IPv6. <ul style="list-style-type: none"> <li><b>default</b>—Set the switch to the default template to balance system resources.</li> <li><b>routing</b>—Set the switch to the routing template to support IPv4 and IPv6 routing, including IPv4 policy-based routing.</li> <li><b>vlan</b>—Maximize VLAN configuration on the switch with no routing supported in hardware.</li> </ul>
Step 3	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>reload</code>	Reload the operating system.
Step 5	<code>configure terminal</code>	Enter global configuration mode after the switch reloads.
Step 6	<code>interface interface-id</code>	Enter interface configuration mode, and specify the Layer 3 interface to configure. The interface can be a physical interface, a switch virtual interface (SVI), or a Layer 3 EtherChannel.
Step 7	<code>no switchport</code>	Remove the interface from Layer 2 configuration mode (if it is a physical interface).
Step 8	<code>ipv6 address ipv6-prefix/prefix length eui-64</code>  or <code>ipv6 address ipv6-address/prefix length</code>  or <code>ipv6 address ipv6-address link-local</code>  or <code>ipv6 enable</code>	Specify 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.  Manually configure an IPv6 address on the interface.  Specify a link-local address on the interface to be used 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.  Automatically configure an IPv6 link-local address on the interface, and enable the interface for IPv6 processing. The link-local address can only be used to communicate with nodes on the same link.
Step 9	<code>exit</code>	Return to global configuration mode.
Step 10	<code>ip routing</code>	Enable IP routing on the switch.
Step 11	<code>ipv6 unicast-routing</code>	Enable forwarding of IPv6 unicast data packets.
Step 12	<code>end</code>	Return to privileged EXEC mode.
Step 13	<code>show ipv6 interface interface-id</code>	Verify your entries.
Step 14	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

To remove an IPv6 address from an interface, use the **no ipv6 address *ipv6-prefix/prefix length eui-64*** or **no ipv6 address *ipv6-address link-local*** interface configuration command. To remove all manually configured IPv6 addresses from an interface, use the **no ipv6 address** interface configuration command without arguments. To disable IPv6 processing on an interface that has not been explicitly configured with an IPv6 address, use the **no ipv6 enable** interface configuration command. To globally disable IPv6 routing, use the **no ipv6 unicast-routing** global configuration command.

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 shows how the interface ID (20B:46FF:FE2F:D940) is appended to the link-local prefix FE80::/64 of the interface.

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
Switch# show ipv6 interface gigabitethernet1/0/1
GigabitEthernet1/0/1 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):
    FE02::1
    FE02::2
    FE02::1:FE2F: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.
```

## Configuring Default Router Preference

Router advertisement messages are sent with the default router preference (DRP) configured by the **ipv6 nd router-preference** interface configuration command. If no DRP is configured, RAs are sent with a medium preference.

A DRP is useful when two routers on a link might provide equivalent, but not equal-cost routing, and policy might dictate that hosts should prefer one of the routers.

Beginning in privileged EXEC mode, follow these steps to configure a DRP for a router on an interface.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface <i>interface-id</i></b>	Enter interface configuration mode, and enter the Layer 3 interface on which you want to specify the DRP.
Step 3	<b>ipv6 nd router-preference {high   medium   low}</b>	Specify a DRP for the router on the switch interface.
Step 4	<b>end</b>	Return to privileged EXEC mode.

	Command	Purpose
Step 5	<code>show ipv6 interface</code>	Verify the configuration.
Step 6	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

Use the **no ipv6 nd router-preference** interface configuration command to disable an IPv6 DRP.

This example shows how to configure a DRP of *high* for the router on an interface.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ipv6 nd router-preference high
Switch(config-if)# end
```

For more information about configuring DRP for IPv6, see the “Implementing IPv6 Addresses and Basic Connectivity” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## Configuring IPv4 and IPv6 Protocol Stacks

Before configuring IPv6 routing, you must select an SDM template that supports IPv4 and IPv6. If not already configured, use the **sdm prefer dual-ipv4-and-ipv6 {default | routing | vlan} [desktop]** global configuration command to configure a template that supports IPv6. When you select a new template, you must reload the switch by using the **reload** privileged EXEC command so that the template takes effect.

Beginning in privileged EXEC mode, follow these steps to configure a Layer 3 interface to support both IPv4 and IPv6 and to enable IPv6 routing.

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip routing</code>	Enable routing on the switch.
Step 3	<code>ipv6 unicast-routing</code>	Enable forwarding of IPv6 data packets on the switch.
Step 4	<code>interface interface-id</code>	Enter interface configuration mode, and specify the Layer 3 interface to configure.
Step 5	<code>no switchport</code>	Remove the interface from Layer 2 configuration mode (if it is a physical interface).
Step 6	<code>ip address ip-address mask [secondary]</code>	Specify a primary or secondary IPv4 address for the interface.
Step 7	<code>ipv6 address ipv6-prefix/prefix length eui-64</code>  or <code>ipv6 address ipv6-address link-local</code> or <code>ipv6 enable</code>	Specify a global IPv6 address. Specify only the network prefix; the last 64 bits are automatically computed from the switch MAC address.  Specify a link-local address on the interface to be used instead of the automatically configured link-local address when IPv6 is enabled on the interface.  Automatically configure an IPv6 link-local address on the interface, and enable the interface for IPv6 processing. The link-local address can only be used to communicate with nodes on the same link.
Step 8	<code>end</code>	Return to privileged EXEC mode.



	Command	Purpose
Step 9	<pre>show interface <i>interface-id</i> show ip interface <i>interface-id</i> show ipv6 interface <i>interface-id</i></pre>	Verify your entries.
Step 10	<pre>copy running-config startup-config</pre>	(Optional) Save your entries in the configuration file.

To disable IPv4 routing, use the **no ip routing** global configuration command. To disable IPv6 routing, use the **no ipv6 unicast-routing** global configuration command. To remove an IPv4 address from an interface, use the **no ip address *ip-address mask*** interface configuration command. To remove an IPv6 address from an interface, use the **no ipv6 address *ipv6-prefix/prefix length eui-64*** or **no ipv6 address *ipv6-address link-local*** interface configuration command. To remove all manually configured IPv6 addresses from an interface, use the **no ipv6 address** interface configuration command without arguments. To disable IPv6 processing on an interface that has not been explicitly configured with an IPv6 address, use the **no ipv6 enable** interface configuration command.

This example shows how to enable IPv4 and IPv6 routing on an interface.

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ip routing
Switch(config)# ipv6 unicast-routing
Switch(config)# interface fastethernet1/0/11
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.99.1 244.244.244.0
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
```

## Configuring DHCP for IPv6 Address Assignment

These sections describe how to configure Dynamic Host Configuration Protocol for IPv6 (DHCPv6) address assignment:

- [Default DHCPv6 Address Assignment Configuration, page 40-17](#)
- [DHCPv6 Address Assignment Configuration Guidelines, page 40-17](#)
- [Enabling DHCPv6 Server Function, page 40-18](#)
- [Enabling DHCPv6 Client Function, page 40-20](#)

### Default DHCPv6 Address Assignment Configuration

By default, no DHCPv6 features are configured on the switch.

### DHCPv6 Address Assignment Configuration Guidelines

When configuring DHCPv6 address assignment, consider these guidelines:

- In the procedures, the specified interface must be one of these Layer 3 interfaces:
  - DHCPv6 IPv6 routing must be enabled on a Layer 3 interface.
  - SVI: a VLAN interface created by using the **interface *vlan* *vlan\_id*** command.
  - EtherChannel port channel in Layer 3 mode: a port-channel logical interface created by using the **interface *port-channel* *port-channel-number*** command.

- Before configuring DHCPv6, you must select a Switch Database Management (SDM) template that supports IPv4 and IPv6.
- The switch can act as a DHCPv6 client, server, or relay agent. The DHCPv6 client, server, and relay function are mutually exclusive on an interface.
- The DHCPv6 client, server, or relay agent runs only on the master switch. When there is a stack master re-election, the new master switch retains the DHCPv6 configuration. However, the local RAM copy of the DHCP server database lease information is not retained.

Beginning with Cisco IOS Release 12.2(58)SE, the switch supports these features:

- DHCPv6 Bulk Lease Query

DHCPv6 bulk-lease query allows a client to request information about DHCPv6 bindings. This functionality adds new query types and allows the bulk transfer of DHCPv6 binding data through TCP. Bulk transfer of DHCPv6 binding data is useful when the relay server switch is rebooted and the relay server has lost all the binding information because after the reboot, the relay server automatically generates a Bulk Lease Query to get the binding information from DHCP server.

- DHCPv6 Relay Source Configuration

The DHCPv6 server replies to the source address of the DHCP relay agent. Typically, messages from a DHCPv6 relay agent show the source address of the interface from which they are sent. However, in some networks, it may be desirable to configure a more stable address (such as a loopback interface) as the source address for messages from the relay agent. The DHCPv6 Relay Source Configuration feature provides this capability.

For more information and to configure these features, see the [Cisco IOS IPv6 Configuration Guide, Release 12.4](#).

## Enabling DHCPv6 Server Function

Beginning in privileged EXEC mode, follow these steps to enable the DHCPv6 server function on an interface.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ipv6 dhcp pool <i>poolname</i></b>	Enter DHCP pool configuration mode, and define the name for the IPv6 DHCP pool. The pool name can be a symbolic string (such as Engineering) or an integer (such as 0).
Step 3	<b>address prefix <i>IPv6-prefix</i> lifetime {<i>t1 t1</i>   infinite}</b>	(Optional) Specify an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons. <b>lifetime <i>t1 t1</i></b> —Specify a time interval (in seconds) that an IPv6 address prefix remains in the valid state. The range is 5 to 4294967295 seconds. Specify <b>infinite</b> for no time interval.
Step 4	<b>link-address <i>IPv6-prefix</i></b>	(Optional) Specify a link-address IPv6 prefix. When an address on the incoming interface or a link-address in the packet matches the specified IPv6 prefix, the server uses the configuration information pool. This address must be in hexadecimal, using 16-bit values between colons.

	Command	Purpose
Step 5	<b>vendor-specific</b> <i>vendor-id</i>	(Optional) Enter vendor-specific configuration mode and enter a vendor-specific identification number. This number is the vendor IANA Private Enterprise Number. The range is 1 to 4294967295.
Step 6	<b>suboption</b> <i>number</i> { <b>address</b> <i>IPv6-address</i>   <b>ascii</b> <i>ASCII-string</i>   <b>hex</b> <i>hex-string</i> }	(Optional) Enter a vendor-specific suboption number. The range is 1 to 65535. Enter an IPv6 address, ASCII text, or a hex string as defined by the suboption parameters.
Step 7	<b>exit</b>	Return to DHCP pool configuration mode.
Step 8	<b>exit</b>	Return to global configuration mode.
Step 9	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the interface to configure.
Step 10	<b>ipv6 dhcp server</b> [ <i>poolname</i>   <b>automatic</b> ] [ <b>rapid-commit</b> ] [ <b>preference</b> <i>value</i> ] [ <b>allow-hint</b> ]	Enable DHCPv6 server function on an interface. <ul style="list-style-type: none"> <li>• <b>poolname</b>—(Optional) User-defined name for the IPv6 DHCP pool. The pool name can be a symbolic string (such as <i>Engineering</i>) or an integer (such as 0).</li> <li>• <b>automatic</b>—(Optional) Enables the system to automatically determine which pool to use when allocating addresses for a client.</li> <li>• <b>rapid-commit</b>—(Optional) Allow two-message exchange method.</li> <li>• <b>preference value</b>—(Optional) The preference value carried in the preference option in the advertise message sent by the server. The range is from 0 to 255. The preference value default is 0.</li> <li>• <b>allow-hint</b>—(Optional) Specifies whether the server should consider client suggestions in the SOLICIT message. By default, the server ignores client hints.</li> </ul>
Step 11	<b>end</b>	Return to privileged EXEC mode.
Step 12	<b>show ipv6 dhcp pool</b>  or <b>show ipv6 dhcp interface</b>	Verify DHCPv6 pool configuration.  Verify that the DHCPv6 server function is enabled on an interface.
Step 13	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To delete a DHCPv6 pool, use the **no ipv6 dhcp pool** *poolname* global configuration command. Use the **no** form of the DHCP pool configuration mode commands to change the DHCPv6 pool characteristics. To disable the DHCPv6 server function on an interface, use the **no ipv6 dhcp server** interface configuration command.

This example shows how to configure a pool called *engineering with an IPv6 address prefix*:

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool engineering
Switch(config-dhcpv6)#address prefix 2001:1000::0/64
Switch(config-dhcpv6)# end
```

This example shows how to configure a pool called *testgroup* with three link-addresses and an IPv6 address prefix:

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool testgroup
Switch(config-dhcpv6)# link-address 2001:1001::0/64
Switch(config-dhcpv6)# link-address 2001:1002::0/64
Switch(config-dhcpv6)# link-address 2001:2000::0/48
Switch(config-dhcpv6)# address prefix 2001:1003::0/64
Switch(config-dhcpv6)# end
```

This example shows how to configure a pool called *350* with vendor-specific options:

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool 350
Switch(config-dhcpv6)# address prefix 2001:1005::0/48
Switch(config-dhcpv6)# vendor-specific 9
Switch(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Switch(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Switch(config-dhcpv6-vs)# end
```

## Enabling DHCPv6 Client Function

Beginning in privileged EXEC mode, follow these steps to enable DHCPv6 client function on an interface.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the interface to configure.
Step 3	<b>ipv6 address dhcp</b> [ <b>rapid-commit</b> ]	Enable the interface to acquire an IPv6 address from the DHCPv6 server. <b>rapid-commit</b> —(Optional) Allow two-message exchange method for address assignment.
Step 4	<b>ipv6 dhcp client request</b> [ <b>vendor-specific</b> ]	(Optional) Enable the interface to request the vendor-specific option.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show ipv6 dhcp interface</b>	Verify that the DHCPv6 client is enabled on an interface.

To disable the DHCPv6 client function, use the **no ipv6 address dhcp** interface configuration command. To remove the DHCPv6 client request, use the **no ipv6 address dhcp client request** interface configuration command.

This example shows how to acquire an IPv6 address and to enable the rapid-commit option:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ipv6 address dhcp rapid-commit
```

This document describes only the DHCPv6 address assignment. For more information about configuring the DHCPv6 client, server, or relay agent functions, see the “Implementing DHCP for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## 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:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ipv6 icmp error-interval</b> <i>interval</i> [ <i>bucketsize</i> ]	Configure the interval and bucket size for IPv6 ICMP error messages: <ul style="list-style-type: none"> <li><i>interval</i>—The interval (in milliseconds) between tokens being added to the bucket. The range is from 0 to 2147483647 milliseconds.</li> <li><i>bucketsize</i>—(Optional) The maximum number of tokens stored in the bucket. The range is from 1 to 200.</li> </ul>
Step 3	<b>end</b>	Return to privileged EXEC mode.
Step 4	<b>show ipv6 interface</b> [ <i>interface-id</i> ]	Verify your entries.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default configuration, use the **no ipv6 icmp error-interval** global configuration command.

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

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

## Configuring CEF and dCEF for IPv6

Cisco Express Forwarding (CEF) is a Layer 3 IP switching technology to improve network performance. In a switch stack, the hardware uses distributed CEF (dCEF) in the stack. IPv6 CEF is IPv6 CEF and dCEF are disabled by default but are automatically enabled when you configure IPv6 routing.

To route IPv6 unicast packets, you must first globally configure IPv6 unicast packet forwarding by using the **ipv6 unicast-routing** global configuration command. You must configure an IPv6 address and IPv6 processing on an interface by using the **ipv6 address** interface configuration command.

To disable IPv6 CEF or distributed CEF, use the **no ipv6 cef** or **no ipv6 cef distributed** global configuration command. To reenab IPv6 CEF or dCEF if it has been disabled, use the **ipv6 cef** or **ipv6 cef distributed** global configuration command. You can verify the IPv6 state by entering the **show ipv6 cef** privileged EXEC command.

For more information about configuring CEF and dCEF, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## Configuring Static Routes for IPv6

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, and enable IPv6 on at least one Layer 3 interface by configuring an IPv6 address on the interface.

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

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ipv6 route</b> <i>ipv6-prefix/prefix length</i> { <i>ipv6-address</i>   <i>interface-id</i> [ <i>ipv6-address</i> ]} [ <i>administrative distance</i> ]	<p>Configure a static IPv6 route.</p> <ul style="list-style-type: none"> <li>• <i>ipv6-prefix</i>—The IPv6 network that is the destination of the static route. It can also be a hostname when static host routes are configured.</li> <li>• <i>/prefix length</i>—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.</li> <li>• <i>ipv6-address</i>—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 specified in hexadecimal using 16-bit values between colons.</li> <li>• <i>interface-id</i>—Specify 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.</li> </ul> <p><b>Note</b> You must specify an <i>interface-id</i> when using a link-local address as the next hop (the link-local next hop must also be an adjacent router).</p> <ul style="list-style-type: none"> <li>• <i>administrative distance</i>—(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.</li> </ul>
Step 3	<b>end</b>	Return to privileged EXEC mode.

	Command	Purpose
Step 4	<pre>show ipv6 static [ipv6-address   ipv6-prefix/prefix length] [interface interface-id] [recursive] [detail]</pre> <p>or</p> <pre>show ipv6 route static [updated]</pre>	<p>Verify your entries by displaying the contents of the IPv6 routing table.</p> <ul style="list-style-type: none"> <li>• <b>interface</b> <i>interface-id</i>—(Optional) Display only those static routes with the specified interface as an egress interface.</li> <li>• <b>recursive</b>—(Optional) Display only recursive static routes. The <b>recursive</b> keyword is mutually exclusive with the <b>interface</b> keyword, but it can be used with or without the IPv6 prefix included in the command syntax.</li> <li>• <b>detail</b>—(Optional) Display this additional information: <ul style="list-style-type: none"> <li>– For valid recursive routes, the output path set, and maximum resolution depth.</li> <li>– For invalid routes, the reason why the route is not valid.</li> </ul> </li> </ul>
Step 5	<pre>copy running-config startup-config</pre>	(Optional) Save your entries in the configuration file.

To remove a configured static route, use the **no ipv6 route** *ipv6-prefix/prefix length {ipv6-address | interface-id [ipv6-address]} [administrative distance]* global configuration command.

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

```
Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet2/0/1 130
```

For more information about configuring static IPv6 routing, see the “Implementing Static Routes for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## Configuring RIP for IPv6

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, and enable IPv6 on any Layer 3 interfaces on which IPv6 RIP is to be enabled.

Beginning in privileged EXEC mode, follow these required and optional steps to configure IPv6 RIP:

	Command	Purpose
Step 1	<pre>configure terminal</pre>	Enter global configuration mode.
Step 2	<pre>ipv6 router rip name</pre>	Configure an IPv6 RIP routing process, and enter router configuration mode for the process.
Step 3	<pre>maximum-paths number-paths</pre>	(Optional) Define the maximum number of equal-cost routes that IPv6 RIP can support. The range is from 1 to 64, and the default is 4 routes.
Step 4	<pre>exit</pre>	Return to global configuration mode.
Step 5	<pre>interface interface-id</pre>	Enter interface configuration mode, and specify the Layer 3 interface to configure.
Step 6	<pre>ipv6 rip name enable</pre>	Enable the specified IPv6 RIP routing process on the interface.

	Command	Purpose
Step 7	<code>ipv6 rip name default-information {only   originate}</code>	(Optional) Originate the IPv6 default route (::/0) in the RIP routing process updates sent from the specified interface.  <b>Note</b> 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.  <ul style="list-style-type: none"> <li>• <b>only</b>—Select to originate the default route, but suppress all other routes in the updates sent on this interface.</li> <li>• <b>originate</b>—Select to originate the default route in addition to all other routes in the updates sent on this interface.</li> </ul>
Step 8	<code>end</code>	Return to privileged EXEC mode.
Step 9	<code>show ipv6 rip [name] [interface interface-id] [database] [next-hops]</code>  or <code>show ipv6 route rip [updated]</code>	Display information about IPv6 RIP processes.  Display the contents of the IPv6 routing table.
Step 10	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

To disable a RIP routing process, use the **no ipv6 router rip name** global configuration command. To disable the RIP routing process for an interface, use the **no ipv6 rip name** interface configuration command.

This example shows how to enable the RIP routing process *cisco* with a maximum of eight equal-cost routes and to enable it on an interface:

```
Switch(config)# ipv6 router rip cisco
Switch(config-router)# maximum-paths 8
Switch(config)# exit
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ipv6 rip cisco enable
```

For more information about configuring RIP routing for IPv6, see the “Implementing RIP for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com

## Configuring OSPF for IPv6

You can customize OSPF for IPv6 for your network. However, the defaults for OSPF in IPv6 are set to meet the requirements of most customers and features.

Follow these guidelines:

- Be careful when changing the defaults for IPv6 commands. Changing the defaults might adversely affect OSPF for the IPv6 network.
- Before you enable IPv6 OSPF on an interface, 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, and enable IPv6 on Layer 3 interfaces on which you are enabling IPv6 OSPF.



Beginning in privileged EXEC mode, follow these required and optional steps to configure IPv6 OSPF:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>ipv6 router ospf</b> <i>process-id</i>	Enable OSPF router configuration mode for the process. The process ID is the number administratively assigned when enabling the OSPF for IPv6 routing process. It is locally assigned and can be a positive integer from 1 to 65535.
Step 3	<b>area</b> <i>area-id</i> <b>range</b> { <i>ipv6-prefix/prefix length</i> } [ <b>advertise</b>   <b>not-advertise</b> ] [ <b>cost</b> <i>cost</i> ]	(Optional) Consolidate and summarize routes at an area boundary. <ul style="list-style-type: none"> <li>• <i>area-id</i>—Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IPv6 prefix.</li> <li>• <i>ipv6-prefix/prefix length</i>—The destination IPv6 network and 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.</li> <li>• <b>advertise</b>—(Optional) Set the address range status to advertise and to generate a Type 3 summary link-state advertisement (LSA).</li> <li>• <b>not-advertise</b>—(Optional) Set the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and component networks remain hidden from other networks.</li> <li>• <b>cost</b> <i>cost</i>—(Optional) Metric or cost for this summary route, which is used during OSPF SPF calculation to determine the shortest paths to the destination. The value can be 0 to 16777215.</li> </ul>
Step 4	<b>maximum paths</b> <i>number-paths</i>	(Optional) Define the maximum number of equal-cost routes to the same destination that IPv6 OSPF should enter in the routing table. The range is from 1 to 64, and the default is 16.
Step 5	<b>exit</b>	Return to global configuration mode.
Step 6	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and specify the Layer 3 interface to configure.
Step 7	<b>ipv6 ospf</b> <i>process-id</i> <b>area</b> <i>area-id</i> [ <b>instance</b> <i>instance-id</i> ]	Enable OSPF for IPv6 on the interface. <b>instance</b> <i>instance-id</i> —(Optional) Instance identifier.
Step 8	<b>end</b>	Return to privileged EXEC mode.
Step 9	<b>show ipv6 ospf</b> [ <i>process-id</i> ] [ <i>area-id</i> ] <b>interface</b> [ <i>interface-id</i> ] or <b>show ipv6 ospf</b> [ <i>process-id</i> ] [ <i>area-id</i> ]	Display information about OSPF interfaces.  Display general information about OSPF routing processes.
Step 10	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To disable an OSPF routing process, use the **no ipv6 router ospf *process-id*** global configuration command. To disable the OSPF routing process for an interface, use the **no ipv6 ospf *process-id* area *area-id*** interface configuration command.

For more information about configuring OSPF routing for IPv6, see the “Implementing OSPF for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## Configuring IPsec on OSPFv3



### Note

To enable authentication and encryption, configure the IP Security (IPsec) secure socket application program interface (API) on OSPFv3.

For information about configuring IPsec, see the following sections of the *Cisco IOS IPv6 Configuration Library* on Cisco.com:

- [Defining Authentication on an Interface](#)
- [Defining Encryption on an Interface](#)
- [Defining Authentication in an OSPFv3 Area](#)
- [Defining Encryption in an OSPFv3 Area](#)
- [Defining Authentication and Encryption for a Virtual Link in an OSPFv3 Area](#)
- [Verifying OSPFv3 Configuration and Operation](#)

## Configuring EIGRP for IPv6

EIGRP for IPv6 is enabled when you configure the **ipv6 router eigrp *as-number*** command and **ipv6 eigrp *as-number*** command on the interface.

To set an explicit router ID, use the **show ipv6 eigrp** command to identify the configured router IDs, and then use the **eigrp router-id *ip-address*** command.

As with EIGRP IPv4, you can use EIGRPv6 to specify your EIGRP IPv4 interfaces and to select a subset of those as passive interfaces. Use the **passive-interface default** command to make all interfaces passive, and then use the **no passive-interface** command on selected interfaces to make them active. EIGRP IPv6 does not need to be configured on a passive interface.

For more configuration procedures, see the “Implementing EIGRP for IPv6” chapter, in the *Cisco IOS IPv6 Configuration Guide*.

## Configuring HSRP for IPv6

Hot Standby Router Protocol (HSRP) for IPv6 provides routing redundancy for routing IPv6 traffic not dependent on the availability of any single router.

When HSRP for IPv6 is enabled on a switch, IPv6 hosts learn of available IPv6 routers through IPv6 neighbor discovery router advertisement messages. An HSRP IPv6 group has a virtual MAC address that is derived from the HSRP group number. The group has a virtual IPv6 link-local address that is, by default, derived from the HSRP virtual MAC address. Periodic messages are sent for the HSRP virtual IPv6 link-local address when the HSRP group is active.

When configuring HSRP for IPv6, you must enable HSRP version 2 (HSRPv2) on the interface. For more information about HSRP for IPv6 and HSRPv2, see the [Chapter 42, “Configuring HSRP and VRRP.”](#)

**Note**

Before configuring an HSRP for IPv6 group, you must enable the forwarding of IPv6 packets by using the **ipv6 unicast-routing** global configuration command and enable IPv6 on the interface on which you will configure an HSRP for IPv6 group.

## Enabling HSRP Version 2

Beginning in privileged EXEC mode, follow these steps to enable HSRP version 2 on a Layer 3 interface.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and enter the Layer 3 interface on which you want to specify the standby version.
Step 3	<b>standby version</b> {1   2}	Enter <b>2</b> to change the HSRP version. The default is 1.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show standby</b>	Verify the configuration.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

## Enabling an HSRP Group for IPv6

Beginning in privileged EXEC mode, follow these steps to create or enable HSRP for IPv6 on a Layer 3 interface.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Enter interface configuration mode, and enter the Layer 3 interface on which you want to enable HSRP for IPv6.
Step 3	<b>standby</b> [ <i>group-number</i> ] <b>ipv6</b> { <i>link-local-address</i>   <b>autoconfig</b> }	Create (or enable) the HSRP for IPv6 group. <ul style="list-style-type: none"> <li>(Optional) <i>group-number</i>—The group number on the interface for which HSRP is being enabled. The range is 0 to 4095. The default is 0. If there is only one HSRP group, you do not need to enter a group number.</li> <li>Enter the link-local address of the Hot Standby router interface, or enable the link-local address to be generated automatically from the link-local prefix and a modified EUI-64 format interface identifier, where the EUI-64 interface identifier is created from the relevant HSRP virtual MAC address.</li> </ul>

	Command	Purpose
Step 4	<code>standby [group-number] preempt [delay {minimum seconds   reload seconds   sync seconds}]</code>	<p>Configure the router to <b>preempt</b>, which means that when the local router has a higher priority than the active router, it assumes control as the active router.</p> <ul style="list-style-type: none"> <li>(Optional) <i>group-number</i>—The group number to which the command applies.</li> <li>(Optional) <b>delay</b>—Set to cause the local router to postpone taking over the active role for the shown number of seconds. The range is 0 to 3600 (1 hour). The default is 0 (no delay before taking over).</li> <li>(Optional) <b>reload</b>—Set the preemption delay, in seconds, after a reload. The delay period applies only to the first interface-up event after the router reloads.</li> <li>(Optional) <b>sync</b>—Set the maximum synchronization period, in seconds, for IP redundancy clients.</li> </ul> <p>Use the <b>no</b> form of the command to restore the default values.</p>
Step 5	<code>standby [group-number] priority priority</code>	<p>Set a <b>priority</b> value used in choosing the active router. The range is 1 to 255; the default priority is 100. The highest number represents the highest priority.</p> <p>Use the <b>no</b> form of the command to restore the default values.</p>
Step 6	<code>end</code>	Return to privileged EXEC mode.
Step 7	<code>show standby [interface-id [group-number]]</code>	Verify the configuration.
Step 8	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

Use the **no standby [group-number] ipv6** interface configuration command to disable HSRP for IPv6.

This example shows how to activate HSRP for IPv6 for group 1 on a port. The IP address used by the hot standby group is learned by using HSRP for IPv6.



#### Note

This procedure is the minimum number of steps required to enable HSRP for IPv6. Other configurations are optional.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ipv6 autoconfig
Switch(config-if)# end
Switch# show standby
```

For more information about configuring HSRP for IPv6, see the “Configuring First Hop Redundancy Protocols in IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

# Displaying IPv6

For complete syntax and usage information on these commands, see the Cisco IOS command reference publications.

Table 40-2 shows the privileged EXEC commands for monitoring IPv6 on the switch.

**Table 40-2** Commands for Monitoring IPv6

Command	Purpose
<code>show ipv6 access-list</code>	Display a summary of access lists.
<code>show ipv6 cef<sup>1</sup></code>	Display Cisco Express Forwarding for IPv6.
<code>show ipv6 interface <i>interface-id</i></code>	Display IPv6 interface status and configuration.
<code>show ipv6 mtu</code>	Display IPv6 MTU per destination cache.
<code>show ipv6 neighbors</code>	Display IPv6 neighbor cache entries.
<code>show ipv6 ospf<sup>1</sup></code>	Display IPv6 OSPF information.
<code>show ipv6 prefix-list</code>	Display a list of IPv6 prefix lists.
<code>show ipv6 protocols<sup>1</sup></code>	Display IPv6 routing protocols on the switch.
<code>show ipv6 rip<sup>1</sup></code>	Display IPv6 RIP routing protocol status.
<code>show ipv6 route<sup>1</sup></code>	Display the IPv6 route table entries.
<code>show ipv6 routers<sup>1</sup></code>	Display the local IPv6 routers.
<code>show ipv6 static</code>	Display IPv6 static routes.
<code>show ipv6 traffic</code>	Display IPv6 traffic statistics.

1. This command is not supported on the Catalyst Switch Module 3012.

Table 40-3 shows the privileged EXEC command for displaying EIGRP IPv6 information.

**Table 40-3** Commands for Displaying EIGRP IPv6 Information

Command	Purpose
<code>show ipv6 eigrp [<i>as-number</i>] <i>interface</i></code>	Displays information about interfaces configured for EIGRP IPv6.
<code>show ipv6 eigrp [<i>as-number</i>] <i>neighbor</i></code>	Displays the neighbors discovered by EIGRP IPv6.
<code>show ipv6 eigrp [<i>as-number</i>] <i>traffic</i></code>	Displays the number of EIGRP IPv6 packets sent and received.
<code>show ipv6 eigrp topology [<i>as-number</i>   <i>ipv6-address</i>] [<i>active</i>   <i>all-links</i>   <i>detail-links</i>   <i>pending</i>   <i>summary</i>   <i>zero-successors</i>]</code>	Displays EIGRP entries in the IPv6 topology table.

Table 40-4 shows the privileged EXEC commands for showing IPv4 and IPv6 address types on the switch.

**Table 40-4** Commands for Displaying IPv4 and IPv6 Address Types

Command	Purpose
<b>show ip http server history</b>	Display the previous 20 connections to the HTTP server, including the IP address accessed and the time when the connection was closed.
<b>show ip http server connection</b>	Display the current connections to the HTTP server, including the local and remote IP addresses being accessed.
<b>show ip http client connection</b>	Display the configuration values for HTTP client connections to HTTP servers.
<b>show ip http client history</b>	Display a list of the last 20 requests made by the HTTP client to the server.

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

```
Switch# 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>
```

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

```
Switch# show ipv6 cef
::/0
  nexthop 3FFE:C000:0:7::777 Vlan7
3FFE:C000:0:1::/64
  attached to Vlan1
3FFE:C000:0:1:20B:46FF:FE2F:D940/128
  receive
3FFE:C000:0:7::/64
  attached to Vlan7
3FFE:C000:0:7::777/128
  attached to Vlan7
3FFE:C000:0:7:20B:46FF:FE2F:D97F/128
  receive
3FFE:C000:111:1::/64
  attached to GigabitEthernet1/0/11
3FFE:C000:111:1:20B:46FF:FE2F:D945/128
  receive
3FFE:C000:168:1::/64
  attached to GigabitEthernet2/0/13
3FFE:C000:168:1:20B:46FF:FE2F:D94B/128
  receive
3FFE:C000:16A:1::/64
  attached to Loopback10
3FFE:C000:16A:1:20B:46FF:FE2F:D900/128
  receive

<output truncated>
```

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

```
Switch# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "rip fer"
  Interfaces:
    Vlan6
  GigabitEthernet2/0/4
  GigabitEthernet2/0/11
  GigabitEthernet1/0/12
  Redistribution:
    None
```

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

```
Switch# show ipv6 rip
RIP process "fer", port 521, multicast-group FF02::9, pid 190
  Administrative distance is 120. Maximum paths is 16
  Updates every 30 seconds, expire after 180
  Holddown lasts 0 seconds, garbage collect after 120
  Split horizon is on; poison reverse is off
  Default routes are not generated
  Periodic updates 9040, trigger updates 60
  Interfaces:
    Vlan6
  GigabitEthernet2/0/4
  GigabitEthernet2/0/11
  GigabitEthernet1/0/12
  Redistribution:
    None
```

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

```
Switch# show ipv6 neighbors
IPv6 Address                               Age Link-layer Addr State Interface
3FFE:C000:0:7::777                         - 0007.0007.0007 REACH V17
3FFE:C101:113:1::33                         - 0000.0000.0033 REACH Fa1/0/13
```

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

```
Switch# show ipv6 static
IPv6 Static routes
Code: * - installed in RIB
* ::/0 via nexthop 3FFE:C000:0:7::777, distance 1
```

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

```
Switch# show ipv6 route
IPv6 Routing Table - 21 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S    ::/0 [1/0]
     via 3FFE:C000:0:7::777
C    3FFE:C000:0:1::/64 [0/0]
     via ::, Vlan1
L    3FFE:C000:0:1:20B:46FF:FE2F:D940/128 [0/0]
     via ::, Vlan1
C    3FFE:C000:0:7::/64 [0/0]
     via ::, Vlan7
L    3FFE:C000:0:7:20B:46FF:FE2F:D97F/128 [0/0]
     via ::, Vlan7
C    3FFE:C000:111:1::/64 [0/0]
     via ::, GigabitEthernet1/0/11
L    3FFE:C000:111:1:20B:46FF:FE2F:D945/128 [0/0]
C    3FFE:C000:168:1::/64 [0/0]
     via ::, GigabitEthernet2/0/4
L    3FFE:C000:168:1:20B:46FF:FE2F:D94B/128 [0/0]
     via ::, GigabitEthernet2/0/4
C    3FFE:C000:16A:1::/64 [0/0]
     via ::, Loopback10
L    3FFE:C000:16A:1:20B:46FF:FE2F:D900/128 [0/0]
     via ::, Loopback10

<output truncated>
```



This is an example of the output from the **show ipv6 traffic** privileged EXEC command.

```
Switch# show ipv6 traffic
IPv6 statistics:
  Rcvd: 1 total, 1 local destination
        0 source-routed, 0 truncated
        0 format errors, 0 hop count exceeded
        0 bad header, 0 unknown option, 0 bad source
        0 unknown protocol, 0 not a router
        0 fragments, 0 total reassembled
        0 reassembly timeouts, 0 reassembly failures
  Sent: 36861 generated, 0 forwarded
        0 fragmented into 0 fragments, 0 failed
        0 encapsulation failed, 0 no route, 0 too big
        0 RPF drops, 0 RPF suppressed drops
  Mcast: 1 received, 36861 sent

ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreachable: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout, 0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        1 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 0 neighbor advert
  Sent: 10112 output, 0 rate-limited
        unreachable: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout, 0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 9944 router advert, 0 redirects
        84 neighbor solicit, 84 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 26749 output

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