Configuring IPv6 Unicast Routing

This chapter describes how to configure IPv6 unicast routing on the Cisco ME 3400E Ethernet Access switch.

For information about configuring IPv4 unicast routing, see Chapter 34, "Configuring IP Unicast Routing." For information on configuring IPv6 access control lists (ACLs) see Chapter 40, "Configuring IPv6 ACLs."

To enable IPv6 routing, you must configure the switch to use the a dual IPv4 and IPv6 switch database management (SDM) template. To configure IPv6 VRF-aware routing, you must use the **dual-ipv4-and-ipv6 routing** template or the **dual-ipv4-and-ipv6 default** template. The **dual-ipv4-and-ipv6 vlan** template does not support VRF-aware routing. See the "Dual IPv4 and IPv6 Protocol Stacks" section on page 38-5.

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

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 IPv6 and other features in this chapter, see these documents.

- For complete syntax and usage information for the commands used in this chapter, see the *Cisco IOS IPv6 Command Reference*:
  http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_book.html
- For all IPv6 configuration information, see the *Cisco IOS IPv6 Configuration Guide, Release 12.4T*
  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4t/ipv6_12_4t_book.html
- You can also use the *Search* field to locate the Cisco IOS software documentation for a specific topic. 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-xml/ios/ipv6/configuration/12-4t/ip6-stat-routes.html

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

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

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 simultaneously forward IPv4 and IPv6 frames at line rate.

128-Bit 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.

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 maximum transmission unit (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

- 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

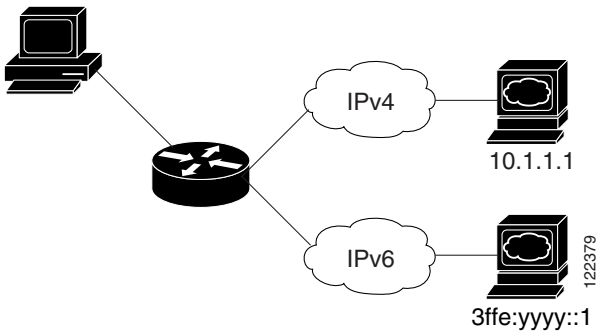
For more information about managing these applications, see the "Managing Cisco IOS Applications over IPv6" chapter and the "Implementing IPv6 Addressing and Basic Connectivity" chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

Dual IPv4 and IPv6 Protocol Stacks

You must use the dual IPv4 and IPv6 template to allocate hardware memory usage to both IPv4 and IPv6 protocols.

Figure 38-1 shows a router forwarding both IPv4 and IPv6 traffic through the same interface, based on the IP packet and destination addresses.

Figure 38-1 Dual IPv4 and IPv6 Support on an Interface



Use the dual IPv4 and IPv6 switch database management (SDM) template to enable IPv6 routing dual stack environments (supporting both IPv4 and IPv6). For more information about the dual IPv4 and IPv6 SDM template, see Chapter 7, "Configuring SDM Templates."

- 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.
- IPv6 QoS is not supported.

- If you do not plan to use IPv6, do not use the dual stack template because it results in less hardware memory availability 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.

Beginning with Cisco IOS Release 12.2(58)SE, switches running the metro IP access image support 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*.

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.

DHCP for IPv6 Server, Client, and Relay

Beginning with Cisco IOS Release 12.2(58)SE, the switch supports IPv6 DHCP in a VRF environment with limited VRF flexibility.

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 Guide* 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.

EIGRP 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.

IS-IS for IPv6

Integrated Intermediate System-to-Intermediate System (IS-IS) for IPv6 is an Interior Gateway Protocol (IGP) that advertises link-state information throughout the network to create a picture of the network topology. IS-IS is an Open Systems Interconnection (OSI) hierarchical routing protocol that designates an intermediate system as a Level 1 or Level 2 device. Level 2 devices route between Level 1 areas to create an intradomain routing backbone. Integrated IS-IS uses a single routing algorithm to support several network address families, such as IPv6, IPv4, and OSI.

For information on configuration procedures, see the "Implementing IS-IS for IPv6" chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-is-is.html

Multiprotocol BGP for IPv6

Multiprotocol Border Gateway Protocol (BGP) is the supported exterior gateway protocol for IPv6. Multiprotocol BGP extensions for IPv6 support the same features and functionality as IPv4 BGP. IPv6 enhancements to multiprotocol BGP include support for IPv6 address family and network layer reachability information (NLRI) and next-hop (the next router in the path to the destination) attributes that use IPv6 addresses.

The switch does not support multicast BGP or non-stop forwarding (NSF) for IPv6 or for BGP IPv6.

For more information about configuring BGP for IPv6, see the “Implementing Multiprotocol BGP for IPv6” chapter in the *Cisco IOS IPv6 Configuration Guide* 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 Guide* 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 Guide* 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 waits 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.

Multi-Protocol VRF (VRF-Lite) for IPv6

The switch supports IPv4 Multi-Protocol VRF-CE (also referred to as VRF-Lite). See the "Configuring Multi-VRF CE" section on page 34-82. Beginning with Cisco IOS Release 12.2(58)SE, the switches running the metro IP access image also support a similar feature for IPv6. IPv6 VRF-Lite supports partial MPLS-VRF PE functionality, which allows overlapping IPv6 unicast addresses across different VRFs. VRF-Lite does not support MPLS label exchange, LDP adjacency, or MPLS labels. Typically VRF-Lite

uses a trunk port between a PE and CE device to extend some MPLS PE functionality to the CE, and then allows multiple customers to share the same CE device. VRF-Lite allows a service provider to support two or more VPNs with overlapping IP addresses using one interface.

The switch supports these VRF-Lite features on all interfaces:

- Configuration of a single VRF for both IPv4 and IPv6 on the same interface
- Static routing and external BGP (eBGP)
- VRF-aware route applications: ping, traceroute, and Telnet
- VPNs that support both IPv4 and IPv6 traffic
- Up to 26 different VRFs. However, the total number of VRF routes supported might be less, depending on the number of interfaces (SVIs or routed ports) per VRF.

The switch does not support these VFR-aware IPv6 protocols: iBGP, OSPFv3, ISIS, EIGRP, or RIP.

To support IPv6 VRF-Lite, the switch must be running either the IPv4-and-IPv6 default SDM template or the IPv4-and-IPv6 routing template. For IPv6 VRF-Lite, the switch supports approximately 500 routes with the IPv4-and-IPv6 default template and 1800 routes with the IPv4-and-IPv6 routing template. Routes that do not fit into the routing table are put in a retry queue. Enter the **show platform ipv6 unicast retry route** privileged EXEC command to see any routes in the retry queue.

The IPv4 Multi-VRF-Lite commands apply only to IPv4 traffic. The IPv6 VRF-Lite commands work with both IPv6 and IPv4 VRF. You can use the same VRF name for IPv4 and IPv6 traffic. If you anticipate the need to add IPv6 traffic to your existing network, you can migrate your IPv4 VRFs to allow IPv6traffic by using the **vrf upgrade-cli multi-af-mode** {**common-policies** | **non-common policies**} [**vrf** *vrf-name*] global configuration command and configuring IPv6 address families.

Note Although you can continue to configure IPv4 VRFs by using the IPv4-specific commands described in the "Configuring Multi-VRF CE" section on page 34-82, we recommend that you use the IPv6 commands to facilitate future compatibility.

See the "Configuring Multi-Protocol VRF for IPv6" section on page 38-37 for the configuring process.

Unsupported IPv6 Unicast Routing Features

- IPv6 policy-based routing
- Full IPv6 virtual private network (VPN) routing and forwarding (VRF) table support

Note The switch supports IPv6 VRF-Lite (Multi-VRF-CE), which is IPv6 VPN in a VRF environment with limited VRF functionality.

- Support for 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
- HSRP for IPv6

Limitations

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

- When using user-network interface (UNI) or enhanced network interface (ENI) ports for any IPv6-related features, you must first globally enable IP routing and IPv6 routing on the switch by entering the **ip routing** and **ipv6 unicast-routing** global configuration commands even if you are not using IPv6 routing.
- 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.

- 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 might be incorrect.
  - When you send RSPAN IPv6-routed packets, the destination MAC address might 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.
- When using IPv6 VRF Lite, the switch supports approximately 500 routes with the IPv4-and-IPv6 default template and 1800 routes with the IPv4-and-IPv6 routing template. Routes that do not fit into the routing table are put in a retry queue.
- IPv6 unicast routing and IPv6 VRF Lite share the same allocation region of TCAM for IPv6 route entries. If IPv6 routing protocols in the IPv6 global table are enabled before IPv6 VRF-Lite, the routing protocols can install so many route entries that IPv6 VRF Lite default routes no longer fit in the TCAM. To ensure that IPv6 VRF Lite functions correctly, you should enter at least one IPv6 **vrf definition** global configuration command with an IPv6 address family before configuring the IPv6 routing protocols and before configuring any IPv6 addresses on any interfaces.

Configuring IPv6

Default IPv6 Configuration

Table 38-1 shows the default IPv6 configuration.

Table 38-1 Default IPv6 Configuration

Feature	Default Setting
SDM template	Default.
IPv6 routing	Disabled globally and on all interfaces.
CEFv6	Disabled (IPv4 CEF is enabled by default). **Note** When IPv6 routing is enabled, CEFv6 is automatically enabled.
IPv6 addresses	None configured.

Configuring IPv6 Addressing and Enabling IPv6 Routing

Follow these rules or limitations when configuring IPv6 on the switch:

- 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 Unicast Routing Features" section on page 38-9.
- 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 FF02:0:0:0:0:1:ff00::/104 for each unicast address assigned to the interface (the address for 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 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	**configure terminal**	Enter global configuration mode.
Step 2	**sdm prefer dual-ipv4-and-ipv6** {**default** | **routing** | **vlan**}	Select an SDM template that supports IPv4 and IPv6. • **default**—Set the switch to the default template to balance system resources. • **routing**—Set the switch to the routing template to support IPv4 and IPv6 routing, including IPv4 policy-based routing. • **vlan**—Maximize VLAN configuration on the switch with no routing supported in hardware.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**reload**	Reload the operating system.
Step 5	**configure terminal**	Enter global configuration mode.
Step 6	**interface** *interface-id*	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	**no switchport**	Remove the interface from Layer 2 configuration mode (if it is a physical interface).

	Command	Purpose
Step 8	**ipv6 address** *ipv6-prefix/prefix length* **eui-64** or **ipv6 address** *ipv6-address/prefix length* or **ipv6 address** *ipv6-address* **link-local** or **ipv6 enable**	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	**exit**	Return to global configuration mode.
Step 10	**ip routing**	Enable IP routing on the switch.
Step 11	**ipv6 unicast-routing**	Enable forwarding of IPv6 unicast data packets.
Step 12	**end**	Return to privileged EXEC mode.
Step 13	**show ipv6 interface** *interface-id*	Verify your entries.
Step 14	**copy running-config startup-config**	(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 is included to show 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 gigabitethernet0/2
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 gigabitethernet0/11
GigabitEthernet0/2 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.
```

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, router advertisements 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	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and enter the Layer 3 interface on which you want to specify the DRP.
Step 3	**ipv6 nd router-preference** {**high** | **medium** | **low**}	Specify a DRP for the router on the switch interface.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show ipv6 interface**	Verify the configuration.
Step 6	**copy running-config startup-config**	(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 gigabitethernet0/1
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**} **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	**configure terminal**	Enter global configuration mode.
Step 2	**sdm prefer dual-ipv4-and-ipv6** {**default** | **routing** | **vlan**}	Select an SDM template that supports IPv4 and IPv6. • **default**—Set the switch to the default template to balance system resources. • **routing**—Set the switch to the routing template to support IPv4 and IPv6 routing, including IPv4 policy-based routing. • **vlan**—Maximize VLAN configuration on the switch with no routing supported in hardware.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**reload**	Reload the operating system.
Step 5	**configure terminal**	Enter global configuration mode.
Step 6	**ip routing**	Enable IPv4 routing on the switch.
Step 7	**ipv6 unicast-routing**	Enable forwarding of IPv6 data packets on the switch.
Step 8	**interface** *interface-id*	Enter interface configuration mode, and specify the Layer 3 interface to configure.
Step 9	**no switchport**	Remove the interface from Layer 2 configuration mode (if it is a physical interface).
Step 10	**ip address** *ip-address mask* [**secondary**]	Specify a primary or secondary IPv4 address for the interface.
Step 11	**ipv6 address** *ipv6-prefix/prefix length* **eui-64** or **ipv6 address** *ipv6-address/prefix length* or **ipv6 address** *ipv6-address* **link-local** or **ipv6 enable**	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 12	**end**	Return to privileged EXEC mode.
Step 13	**show interface** *interface-id* **show ip interface** *interface-id* **show ipv6 interface** *interface-id*	Verify your entries.
Step 14	**copy running-config startup-config**	(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 gigabitethernet0/2
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

Default DHCPv6 Address Assignment Configuration

By default, no Dynamic Host Configuration Protocol for IPv6 (DHCPv6) features are configured on the switch.

DHCPv6 Address Assignment Configuration Guidelines

When configuring a 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.

Enabling the DHCPv6 Server Address-Assignment

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ipv6 dhcp pool** *poolname*	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	**address prefix** *IPv6-prefix* **lifetime** *{t1 t1* | **infinite***}*	(Optional) Specify an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons. **lifetime** *t1 t1*—Specify a time interval (in seconds) that an IPv6 address prefix remains in the valid state. The range is 5 to 4294967295 seconds. Specify **infinite** for no time interval.
Step 4	**link-address** *IPv6-prefix*	(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.
Step 5	**vendor-specific** *vendor-id*	(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	**suboption** *number {***address** *IPv6-address* | **ascii** *ASCII-string* | **hex** *hex-string}*	(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	**exit**	Return to DHCP pool configuration mode.
Step 8	**exit**	Return to global configuration mode.
Step 9	**interface** *interface-id*	Enter interface configuration mode, and specify the interface to configure.

	Command	Purpose
Step 10	**ipv6 dhcp server** [*poolname* | **automatic***]* *[***rapid-commit***]* *[***preference** *value]* *[***allow-hint***]*	Enable the DHCPv6 server function on an interface. • *poolname*—(Optional) User-defined name for the IPv6 DHCP pool. The pool name can be a symbolic string (such as Engineering) or an integer (such as 0). • **automatic**—(Optional) Enables the system to automatically determine which pool to use when allocating addresses for a client. • **rapid-commit**—(Optional) Allow two-message exchange method. • **preference** *value*—(Optional) The preference value carried in the preference option in the advertise message sent by the server. The range is from 0 to 255. The preference value default is 0. • **allow-hint**—(Optional) Specifies whether the server should consider client suggestions in the SOLICIT message. By default, the server ignores client hints.
Step 11	**end**	Return to privileged EXEC mode.
Step 12	**show ipv6 dhcp pool** or **show ipv6 dhcp interface**	Verify DHCPv6 pool configuration. Verify that the DHCPv6 server function is enabled on an interface.
Step 13	**copy running-config startup-config**	(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 the DHCPv6 Client Address Assignment

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and specify the interface to configure.
Step 3	**ipv6 address dhcp** [**rapid-commit**]	Enable the interface to acquire an IPv6 address from the DHCPv6 server. **rapid-commit**—(Optional) Allow two-message exchange method for address assignment.
Step 4	**ipv6 dhcp client request** [**vendor-specific**]	(Optional) Enable the interface to request the vendor-specific option.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show ipv6 dhcp interface**	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 gigabitethernet0/1
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 DHCP Client, Server and Relay Functions

For more information about configuring the DHCPv6 client, server, and relay agent functions, see the “Implementing DHCP for IPv6” chapter in the *Cisco IOS IPv6 Configuration Guide* on Cisco.com.

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-4t/ip6-dhcp.html

In Cisco IOS Release 12.2(58)SE, on the switch has limited VRF flexibility. It supports DHCP VRF-aware configuration in a VRF environment, but operates as VRF-unaware DHCPv6.

Configuration guidelines:

- In the VRF environment, all DHCPv6 server, relay, and client devices are different devices running DHCPv6:
  - The DHCP relay agent forwards client requests to the DHCP server.
  - The DHCP server uses its global configuration pool to respond to the client request.

- The DHCPv6 server can be shared by multiple VRF DHCP clients or by different location VRFs, or each VRF client can use a different DHCPv6 server.
- When you configure this feature, you should perform VRF configuration before you configure DHCPv6 client, server, and relay.

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	**configure terminal**	Enter global configuration mode.
Step 2	**ipv6 icmp error-interval** *interval* [*bucketsize*]	Configure 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. • *bucketsize*—(Optional) The maximum number of tokens stored in the bucket. The range is from 1 to 200.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show ipv6 interface** [*interface-id*]	Verify your entries.
Step 5	**copy running-config startup-config**	(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 for IPv6

Cisco Express Forwarding (CEF) is a Layer 3 IP switching technology, allowing more CPU processing power to be dedicated to packet forwarding. IPv4 CEF is enabled by default. IPv6 CEF is disabled by default, but automatically enabled when you configure IPv6 routing.

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

To disable IPv6 CEF, use the **no ipv6 cef** global configuration command. To reenable IPv6 CEF, use the **ipv6 cef** global configuration command. You can verify the IPv6 state by entering the **show ipv6 cef** privileged EXEC command.

For more information about configuring CEF, 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.
- 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	**configure terminal**	Enter global configuration mode.
Step 2	**ipv6 route** *ipv6-prefix/prefix length* {*ipv6-address* | *interface-id* [*ipv6-address*]} [*administrative distance*]	Configure a static IPv6 route. • *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 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 next hop does not need to be directly connected; recursion finds the IPv6 address of the directly connected next hop. The address must be specified in hexadecimal using 16-bit values between colons. • *interface-id*—Specify direct static routes from point-to-point and broadcast interfaces. On point-to-point interfaces, you do not need to specify the IPv6 address of the next hop. On 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 be an adjacent router. • *administrative distance*—(Optional) An administrative distance. The range is 1 to 254; the default value is 1, which gives static routes precedence over all but connected routes. To configure a floating static route, use an administrative distance greater than that of the dynamic routing protocol.
Step 3	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 4	**show ipv6 static** [*ipv6-address* | *ipv6-prefix/prefix length*] [**interface** *interface-id*] [**recursive**] [**detail**] or **show ipv6 route static** [*updated*]	Verify your entries by displaying the IPv6 routing table. • **interface** *interface-id*—(Optional) Display only those static routes with the specified interface as an egress interface. • **recursive**—(Optional) Display 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 in the command syntax. • **detail**—(Optional) Display 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**	(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 to an interface. The route has an administrative distance of 130:

```
Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet0/1 130
```

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.
- 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	**configure terminal**	Enter global configuration mode.
Step 2	**ipv6 router rip** *name*	Configure an IPv6 RIP routing process, and enter router configuration mode for the process.
Step 3	**maximum-paths** *number-paths*	(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	**exit**	Return to global configuration mode.
Step 5	**interface** *interface-id*	Enter interface configuration mode, and specify the Layer 3 interface to configure.
Step 6	**ipv6 rip** *name* **enable**	Enable the specified IPv6 RIP routing process on the interface.

	Command	Purpose
Step 7	**ipv6 rip** *name* **default-information** {**only** | **originate**}	(Optional) Originate the IPv6 default route (::/0) into the RIP routing process updates sent from the specified interface. **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**	Return to privileged EXEC mode.
Step 9	**show ipv6 rip** [*name*] [**interface** *interface-id*] [**database**] [**next-hops**] or **show ipv6 route rip** [*updated*]	Display information about current IPv6 RIP processes. Display the current contents of the IPv6 routing table.
Step 10	**copy running-config startup-config**	(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 gigabitethernet0/3
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 are set to meet the requirements of most customers and features.

Follow these guidelines:

- Be careful when changing the defaults for IPv6 commands. Doing so 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.
  - 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	**configure terminal**	Enter global configuration mode.
Step 2	**ipv6 router ospf** *process-id*	Enable OSPF router configuration mode for the process. The process ID is the number assigned administratively when enabling the OSPF for IPv6 routing process. It is locally assigned and can be a positive integer from 1 to 65535.
Step 3	**area** *area-id* **range** {*ipv6-prefix/prefix length*} [**advertise** | **not-advertise**] [**cost** *cost*]	(Optional) Consolidate and summarize routes at an area boundary. • *area-id*—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. • *ipv6-prefix/prefix length*—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. • **advertise**—(Optional) Set the address range status to advertise and to generate a Type 3 summary link-state advertisement (LSA). • **not-advertise**—(Optional) Set the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and component networks remain hidden from other networks. • **cost** *cost*—(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.
Step 4	**maximum paths** *number-paths*	(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 paths.
Step 5	**exit**	Return to global configuration mode.
Step 6	**interface** *interface-id*	Enter interface configuration mode, and specify the Layer 3 interface to configure.
Step 7	**ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*]	Enable OSPF for IPv6 on the interface. • **instance** *instance-id*—(Optional) Instance identifier.
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*interface-id*] or **show ipv6 ospf** [*process-id*] [*area-id*]	Display information about OSPF interfaces. Display general information about OSPF routing processes.
Step 10	**copy running-config startup-config**	(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 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 Library* on Cisco.com.

Configuring IS-IS for IPv6

When configuring supported routing protocols in IPv6, you must create the routing process, enable the routing process on interfaces, and customize the routing protocol for your particular network.

Prerequisites

Before configuring the router to run IPv6 IS-IS, globally enable IPv6 using the **ipv6 unicast-routing** global configuration command. For details on basic IPv6 connectivity tasks, refer to *Implementing IPv6 Addressing and Basic Connectivity*.

Restriction

If you are using IS-IS single-topology support for IPv6, IPv4, or both IPv6 and IPv4, you can configure both IPv6 and IPv4 on an IS-IS interface for Level 1, Level 2, or both Level 1 and Level 2. However, if both IPv6 and IPv4 are configured on the same interface, they must be running the same IS-IS level. IPv4 cannot be configured to run on IS-IS Level 1 only on a specified Ethernet interface while IPv6 is configured to run IS-IS Level 2 only on the same Ethernet interface.

Configuring Single-Topology IS-IS for IPv6

Perform this task to create an IPv6 IS-IS process and enable IPv6 IS-IS support on an interface.

Beginning in privileged EXEC mode, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**clns routing**	Enable ISO connectionless routing on the switch.
Step 3	**router isis** *area-tag*	Enable IS-IS for the specified IS-IS routing process, and enter router configuration mode. Set the *area-tag* as a meaningful name for a routing process (for example, isis1). If this argument is not specified, a null tag is assumed, and the process is referenced with a null tag.
Step 4	**net** *network-entity-title*	Configure an IS-IS network entity title (NET) for the routing process. The *network-entity-title* argument defines the area addresses for the IS-IS area and the system ID of the router. **Note** For more details about the format of the network-entity-title argument, refer to the "Configuring ISO CLNS" chapter in the *Cisco IOS ISO CLNS Configuration Guide*.
Step 5	**exit**	Exit router configuration mode and enter global configuration mode.
Step 6	**interface** *type number*	Specify the interface type and number, and enter interface configuration mode.
Step 7	**ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}	Specify the IPv6 network assigned to the interface and enable IPv6 processing on the interface. **Note** 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.
Step 8	**ipv6 router isis** *area-name*	Enable the specified IPv6 IS-IS routing process on an interface.
Step 9	**end**	Return to privileged EXEC mode.
Step 10	**show isis [area tag] database detail**	Verify the IPv6 IS-IS configuration.
Step 11	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Configuring Multitopology IS-IS for IPv6

When multitopology IS-IS for IPv6 is configured, the **transition** keyword allows you to continue working in the single-topology SPF mode of IS-IS IPv6 while updating to multitopology IS-IS. After every switch is configured with the **transition** keyword, you can remove the **transition** keyword on each switch. When transition mode is not enabled, IPv6 connectivity between switches operating in single-topology mode and switches operating in multitopology mode is not possible.

You can continue to use the existing IPv6 topology while upgrading to multitopology IS-IS. The optional **isis ipv6 metric** command allows you to differentiate between link costs for IPv6 and IPv4 traffic when operating in multitopology mode.

Beginning in privileged EXEC mode, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**clns routing**	Enable ISO connectionless routing on the switch.
Step 3	**router isis** *area-tag*	Enable IS-IS for the specified IS-IS routing process, and enter router configuration mode. Set the *area-tag* as a meaningful name for a routing process (for example, isis1). If this argument is not specified, a null tag is assumed, and the process is referenced with a null tag.
Step 4	**metric-style wide [transition] [level-1 | level-2 | level-1-2]**	Configure a switch running IS-IS to generate and accept only new-style Type Length Value (TLV) objects.
Step 5	**address-family ipv6** [**unicast** | **multicast**]	Specify the IPv6 address family, and enter address family configuration mode. **Note** The **unicast** keyword specifies the unicast IPv6 unicast address family. By default, the router is placed in configuration mode for the unicast IPv6 address family if the unicast keyword is not specified with the **address-family ipv6** command.
Step 6	**multi-topology** [**transition**]	Enable multitopology IS-IS for IPv6. **Note** The optional **transition** keyword allows you to continue using single-topology mode while upgrading to multitopology mode.

Customizing IPv6 IS-IS

Perform this task to configure a new administrative distance for IPv6 IS-IS, configure the maximum number of equal-cost paths that IPv6 IS-IS support, configure summary prefixes for IPv6 IS-IS, and configure an IS-IS instance to advertise the default IPv6 route (::/0). It also explains how to configure the hold-down period between partial route calculations (PRCs) and how often Cisco IOS software performs the SPF calculation when using multitopology IS-IS.

You can customize IS-IS multitopology for IPv6 for your network, but you likely will not need to do so. The defaults for this feature are set to meet the requirements of most customers and features. If you change the defaults, refer to the IPv4 configuration guide and the IPv6 command reference to find the appropriate syntax.

Beginning in privileged EXEC mode, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**clns routing**	Enable ISO connectionless routing on the switch.

	Command	Purpose
Step 3	**router isis** *area-tag*	Enable IS-IS for the specified IS-IS routing process, and enter router configuration mode. Set the *area-tag* as a meaningful name for a routing process (for example, isis1). If this argument is not specified, a null tag is assumed, and the process is referenced with a null tag.
Step 4	**address-family ipv6 [unicast | multicast]**	Specify the IPv6 address family, and enters address family configuration mode. The **unicast** keyword specifies the unicast IPv6 unicast address family. By default, the switch is placed in configuration mode for the unicast IPv6 address family if the **unicast** keyword is not specified with the **address-family ipv6** command.
Step 5	**default-information originate** [**route-map** *map-name*]	(Optional) Inject a default IPv6 route into an IS-IS routing domain. The **route-map** keyword and *map-name* argument specify the conditions under which the IPv6 default route is advertised. If the **route map** keyword is omitted, the IPv6 default route is unconditionally advertised at Level 2.
Step 6	**distance** *value*	(Optional) Define an administrative distance for IPv6 IS-IS routes in the IPv6 routing table. The *value* argument is an integer from 10 to 254. (The values 0 to 9 are reserved for internal use).
Step 7	**maximum-paths** *number-paths*	(Optional) Define the maximum number of equal-cost routes that IPv6 IS-IS can support. This command also supports IPv6 BGP and RIP. The *number-paths* argument is an integer from 1 to 64. The default for BGP is one path; the default for IS-IS and RIP is 16 paths.
Step 8	**summary-prefix** *ipv6-prefix*/*prefix-length* [**level-1 | level-1-2 | level-2**]	(Optional) Allow a Level 1-2 router to summarize Level 1 prefixes at Level 2, instead of advertising the Level 1 prefixes directly when the switch advertises the summary. The *ipv6-prefix* argument in the **summary-prefix** command must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. The *prefix-length* argument is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
Step 9	**prc-interval seconds** [*initial-wait*] [*secondary-wait*]	(Optional) Configure the hold-down period between PRCs for multitopology IS-IS for IPv6.
Step 10	**spf-interval** [**level-1 | level-2**] **seconds** [*initial-wait*] [*secondary-wait*]	(Optional) Configure how often Cisco IOS software performs the SPF calculation for multitopology IS-IS for IPv6.

	Command	Purpose
Step 11	exit	Exit router configuration mode and enter global configuration mode.
Step 12	**interface** *type number*	Specify the interface type and number, and enter interface configuration mode.
Step 13	**isis ipv6 metric** *metric-value* [**level-1** | **level-2** | **level-1-2**]	(Optional) Configure the value of a multitopology IS-IS for IPv6 metric.

Redistributing Routes into an IPv6 IS-IS Routing Process

Beginning in privileged EXEC mode, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**clns routing**	Enable ISO connectionless routing on the switch.
Step 3	**router isis** *area-tag*	Enable IS-IS for the specified IS-IS routing process, and enter router configuration mode. Set the *area-tag* as a meaningful name for a routing process (for example, isis1). If this argument is not specified, a null tag is assumed, and the process is referenced with a null tag.
Step 4	**address-family ipv6 [unicast | multicast]**	Specify the IPv6 address family, and enters address family configuration mode. The **unicast** keyword specifies the unicast IPv6 unicast address family. By default, the switch is placed in configuration mode for the unicast IPv6 address family if the **unicast** keyword is not specified with the **address-family ipv6** command.
Step 5	**redistribute** *source-protocol* [*process-id*] [**include-connected**] [*target-protocol-options*] [*source-protocol-options*]	Redistribute routes from the specified protocol into the IS-IS process. The *source-protocol* argument can be one of the following keywords: • bgp • connected • isis • rip • static Only the arguments and keywords relevant to this task are specified here.

Redistributing IPv6 IS-IS Routes Between IS-IS Levels

Perform this task to redistribute IPv6 routes learned at one IS-IS level into a different level.

Beginning in privileged EXEC mode, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**clns routing**	Enable ISO connectionless routing on the switch.
Step 3	**router isis** *area-tag*	Enable IS-IS for the specified IS-IS routing process, and enter router configuration mode. Set the *area-tag* as a meaningful name for a routing process (for example, isis1). If this argument is not specified, a null tag is assumed, and the process is referenced with a null tag.
Step 4	**address-family ipv6 [unicast | multicast]**	Specify the IPv6 address family, and enters address family configuration mode. The **unicast** keyword specifies the unicast IPv6 unicast address family. By default, the switch is placed in configuration mode for the unicast IPv6 address family if the **unicast** keyword is not specified with the **address-family ipv6** command.
Step 5	**redistribute isis** [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} **distribute-list** *list-name*	Redistribute IPv6 routes from one IS-IS level into another IS-IS level. By default, the routes learned by Level 1 instances are redistributed by the Level 2 instance. **Note** The **protocol** keyword must be **isis** in this configuration of the redistribute command. Only the arguments and keywords relevant to this task are specified here.

Disabling IPv6 Protocol-Support Consistency Checks

Perform this task to disable protocol-support consistency checks in IPv6 single-topology mode.

For single-topology IS-IS IPv6, switches must be configured to run the same set of address families. IS-IS performs consistency checks on hello packets and rejects hello packets that do not have the same set of configured address families. For example, a switch running IS-IS for both IPv4 and IPv6 does not form an adjacency with a switch running IS-IS for IPv4 or IPv6 only. To allow adjacency to be formed in mismatched address-families network, the **adjacency-check** command in IPv6 address family configuration mode must be disabled.

Note Entering the **no adjacency-check** command can adversely affect your network configuration. Enter the **no adjacency-check** command only when you are running IPv4 IS-IS on all of your switches, and you want to add IPv6 IS-IS to your network but need to maintain all your adjacencies during the transition. When the IPv6 IS-IS configuration is complete, remove the **no adjacency-check** command from the configuration.

Beginning in privileged EXEC mode, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**clns routing**	Enable ISO connectionless routing on the switch.
Step 3	**router isis** *area-tag*	Enable IS-IS for the specified IS-IS routing process, and enter router configuration mode. Set the *area-tag* as a meaningful name for a routing process (for example, isis1). If this argument is not specified, a null tag is assumed, and the process is referenced with a null tag.
Step 4	**address-family ipv6 [unicast | multicast]**	Specify the IPv6 address family, and enters address family configuration mode. The **unicast** keyword specifies the unicast IPv6 unicast address family. By default, the switch is placed in configuration mode for the unicast IPv6 address family if the **unicast** keyword is not specified with the **address-family ipv6** command.
Step 5	**no adjacency-check**	Disable the IPv6 protocol-support consistency checks performed on hello packets, allowing IPv6 to be introduced into an IPv4-only network without disrupting existing adjacencies. The **adjacency-check** command is enabled by default.

Configuration Examples for IPv6 IS-IS

Example: Configuring Single-Topology IS-IS for IPv6

The following example enables single-topology mode, creates an IS-IS process, defines the NET, configures an IPv6 address on an interface, and configures the interface to run IPv6 IS-IS:

```
ipv6 unicast-routing

!

router isis isis1

 net 49.0001.0000.0000.000c.00

 exit

interface Ethernet0/0/1

 ipv6 address 2001:DB8::3/64

 ipv6 router isis area2
```

Example: Customizing IPv6 IS-IS

The following example advertises the IPv6 default route (::/0)—with an origin of Ethernet interface 0/0/1—with all other routes in router updates sent on Ethernet interface 0/0/1. This example also sets an administrative distance for IPv6 IS-IS to 90, defines the maximum number of equal-cost paths that IPv6 IS-IS will support as 3, and configures a summary prefix of 2001:DB8::/24 for IPv6 IS-IS.

```
router isis isis1
 address-family ipv6
 default-information originate
 distance 90
 maximum-paths 3
 summary-prefix 2001:DB8::/24
 prc-interval 30 80
 spf-interval level-1 40 90
 exit
```

Example: Redistributing Routes into an IPv6 IS-IS Routing Process

The following example redistributes IPv6 BGP routes into the IPv6 IS-IS Level 2 routing process:

```
router isis isis1
 address-family ipv6
 redistribute bgp 64500 metric 100 route-map isismap
 exit
```

Example: Redistributing IPv6 IS-IS Routes Between IS-IS Levels

The following example redistributes IPv6 IS-IS Level 1 routes into the IPv6 IS-IS Level 2 routing process:

```
router isis isis1
 address-family ipv6
 redistribute isis level-1 into level-2 distribute-list list1
```

Example: Disabling IPv6 Protocol-Support Consistency Checks

The following example disables the adjacency-check command to allow a network administrator to configure IPv6 IS-IS on the router without disrupting the existing adjacencies:

```
router isis isis1
 address-family ipv6
 no adjacency-check
```

Example: Configuring Multitopology IS-IS for IPv6

The following example configures multitopology IS-IS in IPv6 after you have configured IS-IS for IPv6:

```
router isis
 metric-style wide
 address-family ipv6
 multi-topology
```

Example: Configuring the IS-IS IPv6 Metric for Multitopology IS-IS

The following example sets the value of an IS-IS IPv6 metric to 20:

```
interface Ethernet 0/0/1
 isis ipv6 metric 20
```

Verifying IPv6 IS-IS Configuration and Operation

Use the following commands privileged EXEC mode to verify IPv6 IS-IS configurations:

Command	Purpose
show ipv6 protocols [summary]	Display the parameters and current state of the active IPv6 routing processes.
show isis [*process-tag*] [**ipv6** | *****] **topology**	Display a list of all connected switches running IS-IS in all areas.
show clns [*process-tag*] **neighbors** [*interface-type interface-number*] [**area**] [**detail**]	Display end system (ES), intermediate system (IS), and multitopology IS-IS (M-ISIS) neighbors.
show clns *area-tag* **is-neighbors** [*type number*] [**detail**]	Displays IS-IS adjacency information for IS-IS neighbors. Use the **detail** keyword to display the IPv6 link-local addresses of the neighbors.
show isis [**process-tag**] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**]	Display the IS-IS link-state database. The contents of each LSP are displayed using the **detail** keyword.
show isis ipv6 rib [*ipv6-prefix*]	Display the IPv6 local RIB.

Examples

In the following example, output information about the parameters and current state of that active IPv6 routing processes is displayed using the **show ipv6 protocols** command:

```
Switch# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"

  Interfaces:
```

```
    Ethernet0/0/3

    Ethernet0/0/1

    Serial1/0/1

    Loopback1 (Passive)

    Loopback2 (Passive)

    Loopback3 (Passive)

    Loopback4 (Passive)

    Loopback5 (Passive)

  Redistribution:

    Redistributing protocol static at level 1

  Address Summarization:

    L2: 2001:DB8:33::/16  advertised with metric 0

    L2: 2001:DB8:44::/16  advertised with metric 20

    L2: 2001:DB8:66::/16  advertised with metric 10

    L2: 2001:DB8:77::/16  advertised with metric 10
```

In the following example, output information about all connected switches running IS-IS in all areas is displayed using the **show isis topology** command:

```
Switch# show isis topology
IS-IS paths to level-1 routers

System Id       Metric  Next-Hop        Interface       SNPA

0000.0000.000C

0000.0000.000D  20      0000.0000.00AA  Se1/0/1         *HDLC*

0000.0000.000F  10      0000.0000.000F  Et0/0/1         0050.e2e5.d01d

0000.0000.00AA  10      0000.0000.00AA  Se1/0/1         *HDLC*


IS-IS paths to level-2 routers

System Id       Metric  Next-Hop        Interface       SNPA

0000.0000.000A  10      0000.0000.000A  Et0/0/3         0010.f68d.f063

0000.0000.000B  20      0000.0000.000A  Et0/0/3         0010.f68d.f063

0000.0000.000C  --

0000.0000.000D  30      0000.0000.000A  Et0/0/3         0010.f68d.f063

0000.0000.000E  30      0000.0000.000A  Et0/0/3         0010.f68d.f063
```

In the following example, output information to confirm that the local switch has formed all the necessary IS-IS adjacencies with other IS-IS neighbors is displayed using the **show clns is-neighbors** command. To display the IPv6 link-local addresses of the neighbors, specify the **detail** keyword.

Switch# **show clns is-neighbors detail**

```
Tag isis1:
System Id Interface State Type Priority Circuit Id Format
ME3400G-R8 Gi0/3 Up L2 64 ME3400EG-R5.02 Phase V
Area Address(es): 49.0001
IPv6 Address(es): FE80::219:55FF:FE2C:2B43
Uptime: 17:34:26
NSF capable
Interface name: GigabitEthernet0/3
```

In the following example, detailed output information that displays both end system (ES) and intermediate system (IS) neighbors is displayed using the s**how clns neighbors** command with the **detail** keyword.

Switch# **show clns neighbors detail**

```
Tag isis1:
System Id Interface SNPA State Holdtime Type Protocol
ME3400G-R8 Gi0/3 0019.552c.2b43 Up 28 L2 IS-IS
Area Address(es): 49.0001
IPv6 Address(es): FE80::219:55FF:FE2C:2B43
Uptime: 17:21:38
NSF capable
Interface name: GigabitEthernet0/3
```

In the following example, detailed output information about LSPs received from other switches and the IPv6 prefixes they are advertising is displayed using the **show isis database** command with the **detail** keyword specified:

Are these addresses private? Our guidelines are to include IP address as in the other examples.

```
Switch# show isis database detail
Tag isis1:
IS-IS Level-2 Link State Database:
LSPID LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ME3400G-R8.00-00 0x00000625 0xBD91 860 0/0/0
Area Address: 49.0001
NLPID: 0x8E
Hostname: ME3400G-R8
IPv6 Address: 2004::1
Metric: 10 IS ME3400EG-R5.02
Metric: 10 IPv6 2004::/64
ME3400EG-R5.00-00 * 0x00000631 0x938D 1191 0/0/0
Area Address: 49.0001
NLPID: 0x81 0xCC 0x8E
Hostname: ME3400EG-R5
IPv6 Address: 2006::2
Metric: 10 IS ME3400EG-R5.02
Metric: 10 IPv6 2004::/64
Metric: 10 IPv6 2006::/64
ME3400EG-R5.02-00 * 0x00000622 0xFA9E 529 0/0/0
Metric: 0 IS ME3400EG-R5.00
Metric: 0 IS ME3400G-R8.00
```

The following example shows output from the **show isis ipv6 rib** command. An asterisk (*) indicates prefixes that have been installed in the master IPv6 RIB as IS-IS routes. Following each prefix is a list of all paths in order of preference, with optimal paths listed first followed by suboptimal paths.

```
Switch# show isis ipv6 rib
IS-IS IPv6 process "", local RIB

  2001:DB8:88:1::/64

    via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L2  metric 20 LSP [3/7]

    via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L2  metric 20 LSP [3/7]

* 2001:DB8:1357:1::/64

    via FE80::202:7DFF:FE1A:9471/Ethernet2/1, type L2  metric 10 LSP [4/9]

* 2001:DB8:45A::/64

    via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L1  metric 20 LSP [C/6]

    via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L1  metric 20 LSP [C/6]

    via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L2  metric 20 LSP [3/7]

    via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L2  metric 20 LSP [3/7]
```

Configuring BGP for IPv6

When configuring multiprotocol BGP extensions for IPv6, you must create the BGP routing process, configure peering relationships, and customize BGP for your particular network. Note that BGP functions the same in IPv6 as in IPv4. Before configuring the router to run BGP for IPv6, you must use the **ipv6 unicast-routing** command to globally enable IPv6 routing.

Beginning in privileged EXEC mode, follow these steps to configure IPv6 BGP:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**router bgp** *as-number*	Configure a BGP routing process, and enter BGP router configuration mode for the autonomous system number.
Step 3	**no bgp default ipv4-unicast**	Disable the IPv4 unicast address family for the BGP routing process specified in the previous step. Routing information for the IPv4 unicast address family is advertised by default for each BGP routing session unless you enter this command before configuring the **neighbor remote-as** command.
Step 4	**bgp router-id** *ip-address*	(Optional) Configure a fixed 32-bit router ID as the identifier of the local router running BGP. By default, the router ID is the IPv4 address of a router loopback interface. On a router enabled only for IPv6 (no IPv4 address), you must manually configure the BGP router ID. **Note** Configuring a router ID by using this command resets all active BGP peering sessions.

	Command	Purpose
Step 5	***neighbor*** {*ip-address* | *ipv6-address*[%] *interface-type interface-number* | *peer-group-name*} ***remote-as*** *as-number*	Add the IPv6 address of the neighbor in the specified autonomous system to the IPv6 multiprotocol BGP neighbor table of the local router. **Note** The *ipv6-address* must be in hexadecimal, using 16-bit values between colons.
Step 6	**address-family ipv6**	Specify the IPv6 address family and enter address family configuration mode
Step 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**	Enable the neighbor to exchange prefixes for the IPv6 address family with the local router.
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**show bgp ipv6**	Display information about IPv6 BGP configuration.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

For more configuration procedures, see the "Implementing Multiprotocol BGP for IPv6" chapter in the *Cisco IOS IPv6 Configuration Guide* on Cisco.com.

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4/ipv6_12_4_book.html

The switch does not support multicast IPv6 BGP, nonstop forwarding (NSF) for IPv6 BGP, 6PE multipath (EoMPLS), or IPv6 VRF.

Configuring Multi-Protocol VRF for IPv6

To support IPv6 VRF-Lite, the switch must be running the IP access image and either the IPv4-and-IPv6 default SDM template or the IPv4-and-IPv6 routing template.

Note Because some IPv6 indirect routes can use more than one TCAM entry, the total number of supported indirect routes might be less than that shown in the template. If the limit of TCAM entries for IPv6 routes is exceeded, an error message is generated.

Configuring VRF-Lite includes these steps:

- Configure IPv6 VRFs.

  Enter the **vrf definition** *vrf-name* global configuration command to enter VRF configuration mode and to configure the VRF.

- Associate interfaces (for customer VPNs and PE devices) to the defined VRFs.

  In interface configuration mode, enter the **vrf forwarding** *vrf-name* command to bind the VRF to the interface.

- Populate the VRF with static routes or eBGP routes.

For complete information about the commands in this section, see the *Cisco IOS IPv6 Command Reference* at:
http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_book.html

The IPv4 Multi-VRF-Lite commands apply only to IPv4 traffic. The IPv6 VRF-Lite commands work with both IPv6 and IPv4 VRF. You can use the same VRF name for IPv4 and IPv6 traffic. If you anticipate the need to add IPv6 traffic to your existing network, you can migrate your IPv4 VRFs to allow IPv6traffic by using the **vrf upgrade-cli multi-af-mode** {**common-policies** | **non-common policies**} [**vrf** *vrf-name*] global configuration command and configuring IPv6 address families.

Note Although you can continue to use the IPv4-specific commands to configure IPv4 VRFs, using the IPv6 commands allows you to configure both IPv4 and IPv6 VRFs. We recommend that you use the IPv6 commands to facilitate future compatibility.

Beginning in privileged EXEC mode, follow these steps to configure one or more IPv6 VRFs.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**sdm prefer dual-ipv4-and-ipv6** {**default** | **routing**}	Select an SDM template that supports IPv4 and IPv6 routing. • **default**—Set the switch to the default template to balance system resources. This template supports approximately 500 IPv6 VRF routes. • **routing**—Set the switch to the routing template to support IPv4 and IPv6 routing, including IPv4 policy-based routing. This template supports approximately 1800 IPv6 VRF routes.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**reload**	Reload the operating system.
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip routing**	Enable IP routing.
Step 3	**ipv6 unicast-routing**	Enable IPv6 routing.
Step 4	**vrf definition** *vrf-name*	Configure a VPN VRF and enter VRF configuration mode.
Step 5	**rd** *route-distinguisher*	Create a VRF table by specifying a route distinguisher for the VRF. Enter either an AS number and an arbitrary number (xxx:y) or an IP address and arbitrary number (A.B.C.D:y)
Step 6	**route-target** {**export** | **import** | **both**} *route-target-ext-community*	Specify the route target communities for IPv4 and IPv6. Enter either an AS system number and an arbitrary number (xxx:y) or an IP address and an arbitrary number (A.B.C.D:y). The *route-target-ext-community* must be the same as the *route-distinguisher* entered in Step 5.
Step 7	**address-family ipv4**	Enter address family configuration mode to configure an IPv4 routing session.
Step 8	**route-target** {**export** | **import** | **both**} *route-target-ext-community*	Specify the route target communities specific to IPv4.
Step 9	**exit**	Exit IPv4 address family configuration mode
Step 10	**address-family ipv6**	Enter address family configuration mode to configure an IPv6 routing sessions.
Step 11	**route-target** {**export** | **import** | **both**} *route-target-ext-community*	Specify the route target communities specific to IPv6.

	Command	Purpose
Step 12	**exit**	Exit IPv4 address family configuration mode
Step 13	**exit**	Exit VRF configuration mode
Step 14	**interface** *interface-id*	Enter interface configuration mode and specify the Layer 3 interface to be associated with the VRF. The interface can be a routed port or SVI.
Step 15	**vrf forwarding** *vrf-name*	Associate the VRF with the Layer 3 interface.
Step 16	**end**	Return to privileged EXEC mode.
Step 17	**show vrf**	Verify the configuration. Display information about the configured VRFs.
Step 18	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no vrf definition** *vrf-name* global configuration command to delete a VRF and to remove all interfaces from it. Use the **no vrf forwarding** interface configuration command to remove an interface from the VRF.

This example shows the steps required for configuring IPv6 VRF Lite. It requires that the IPv4 and IPv6 default or routing template be configured.

Enable IPv6 VRF Lite:

```
Switch(config)# ip routing
Switch(config)# ipv6 unicast-routing
Switch(config)# vrf definition abc
Switch(config-vrf)# rd 100:2
Switch(config-vrf)# address-family ipv4
Switch(config-vrf-af)# exit
Switch(config-vrf)# address-family ipv6
Switch(config-vrf-af)# exit
Switch(config-vrf)# exit
```

Associate the VRF with a routed interface:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# vrf forwarding abc
Switch(config-if)# no switchport
Switch(config-if)# no ip address
Switch(config-if)# ipv6 address 2000::1/64
Switch(config-if)# exit
```

Associate the VRF with an SVI interface:

```
Switch(config)# vlan 200
Switch(config-vlan)# exit
Switch(config)# interface vlan 200
Switch(config-if)# vrf forwarding abc
Switch(config-if)# no ip address
Switch(config-if)# ipv6 address 2000::1/64
Switch(config-if)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk allowed vlan 200
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
```

Enable BGP routing protocol for IPv6 VRF Lite:

```
Switch(config)# router bgp 1
Switch(config-router)# bgp router-id 1.1.1.1
Switch(config-router)# address-family ipv6 vrf ABC
Switch(config-router-af)# redistribute connected
```

```
Switch(config-router-af)# neighbor 2000::2 remote-as 1
Switch(config-router-af)# neighbor 2000::2 activate
Switch(config-router-af)# exit
Switch(config-router)# exit
Switch(config)# ipv6 route vrf ABC 4000::/64 5000::1
```

Note The last command configures a static route pointing to the customer router.

Verify connectivity:

```
Switch# ping vrf abc 2000::2
Switch# telnet 2222::2 /vrf abc
Switch# traceroute vrf abc2222::2
```

Displaying IPv6

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

Table 38-2 Commands for Monitoring IPv6

Command	Purpose
show bgp ipv6	Display BGP IPv6 configuration and routing tables.
show ipv6 access-list	Display IPv6 access lists.
show ipv6 cef	Display Cisco Express Forwarding for IPv6.
show ipv6 interface *interface-id*	Display IPv6 interface status and configuration.
show ipv6 mtu	Display IPv6 MTU per destination cache.
show ipv6 neighbors	Display IPv6 neighbor cache entries.
show ipv6 ospf	Display IPv6 OSPF information.
show ipv6 prefix-list	Display IPv6 prefix lists.
show ipv6 protocols	Display IPv6 routing protocols on the switch.
show ipv6 rip	Display IPv6 RIP routing protocol status.
show ipv6 route	Display IPv6 route table entries.
show ipv6 routers	Display local IPv6 routers.
show ipv6 static	Display IPv6 static routes.
show ipv6 traffic	Display IPv6 traffic statistics.
show vrf	Display information about VRF configured on the swtich.

Table 38-3 Commands for Displaying EIGRP IPv6 Information

Command	Purpose
show ipv6 eigrp [*as-number*] *interface*	Display information about interfaces configured for EIGRP IPv6.
show ipv6 eigrp [*as-number*] *neighbor*	Display the neighbors discovered by EIGRP IPv6.

Table 38-3 Commands for Displaying EIGRP IPv6 Information (continued)

Command	Purpose
show ipv6 eigrp [*as-number*] *traffic*	Display the number of EIGRP IPv6 packets sent and received.
show ipv6 eigrp topology [*as-number* | *ipv6-address*] [**active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors**]	Display EIGRP entries in the IPv6 topology table.

Table 38-4 Commands for Displaying IPv4 and IPv6 Address Types

Command	Purpose
show ip http server history	Display the previous 20 connections to the HTTP server, including the IP address accessed and the time when the connection was closed.
show ip http server connection	Display the current connections to the HTTP server, including the local and remote IP addresses being accessed.
show ip http client connection	Display the configuration values for HTTP client connections to HTTP servers.
show ip http client history	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 GigabitEthernet0/11
3FFE:C000:111:1:20B:46FF:FE2F:D945/128
  receive
3FFE:C000:168:1::/64
  attached to GigabitEthernet0/43
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
GigabitEthernet0/4
GigabitEthernet0/11
GigabitEthernet0/12
  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
GigabitEthernet0/4
GigabitEthernet0/11
GigabitEthernet0/12
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 Vl7
3FFE:C101:113:1::33                         - 0000.0000.0033  REACH Gi0/13
```

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 ::, GigabitEthernet0/11
L   3FFE:C000:111:1:20B:46FF:FE2F:D945/128 [0/0]
C   3FFE:C000:168:1::/64 [0/0]
     via ::, GigabitEthernet0/4
L   3FFE:C000:168:1:20B:46FF:FE2F:D94B/128 [0/0]
     via ::, GigabitEthernet0/4
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
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        1 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 0 neighbor advert
  Sent: 10112 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 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
```

This is an example of the output from the **show vrf** privileged EXEC command showing IPv4 and IPv6 VRFs:

```
Switch# show vrf brief
  Name                             Default RD          Protocols   Interfaces
  A                                100:1               ipv4
                                                                   Fa1/0/10
                                                                   Vl200
  ABC                              100:2               ipv4,ipv6   Fa1/0/3
  B                                100:3               ipv4
```