CHAPTER 57

Support for IPv6

This chapter lists the IP version 6 (IPv6) features supported on the Catalyst 4500 and Catalyst 4900 series switches.

The IPv6 for Cisco IOS software feature documentation provides implementation and command reference information for IPv6 features supported in the Cisco IOS software. Not all IPv6 features are supported on the Catalyst 4500 and Catalyst 4900 series switches. We strongly recommend that you read this entire chapter before reading the other IPv6 for Cisco IOS software feature documentation.

The *Cisco IOS IPv6 Configuration Guide* is located at the following website:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2s/ip6-15-2s-book.html

The *Cisco IOS IPv6 Command Reference* is located at the following web site:

http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_book.html

This chapter consists of these sections:

Finding Feature Information

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on Cisco.com is not required.

About IPv6

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

For information about how Cisco Systems implements IPv6, go to this URL:

http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

This section describes the features that are supported for IPv6:

IPv6 Addressing and Basic Connectivity

The switch supports only IPv6 unicast addresses. It does not support site-local unicast 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*. it is an example of an IPv6 address:

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

The leading zeros in each field are optional, implementation is easier without them. it 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

The switch supports the following features:

- IPv6 address types: Anycast
- IPv6 default router preferences
- IPv6 MTU path discovery
- Neighbor discovery duplicate address detection
- Cisco Discovery Protocol — IPv6 address family support for neighbor information
- ICMPv6 redirect
- ICMP rate limiting
- DNS lookups over an IPv6 transport
- uRPF
- ICMPv6
- AAAA DNS lookups over an IPv4 transport

You can find information about these features at this location:

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

DHCP

The following DHCP features are supported for IPv6 on the Catalyst 4500 series switch:

- Relay agent
- Relay agent notification for prefix delegation
- Reload persistent interface ID option
- Ethernet remote ID option
- Stateless auto-configuration

You can find information about these features at this location:

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

Security

The following security features are supported for IPv6 on the Catalyst 4500 series switch:

- Secure Shell (SSH) support over IPv6
- Traffic filters
- standard access control lists (ACL)
- extended access control lists
- ACL accounting
- ACL addressing
- ACL DSCP
- ACL flags
- ACL flows
- ACL fragments
- ACL ICMP codes
- ACL logging
- ACL protocols

You can find information about these features at this location:

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

First-Hop Security

The following First-Hop Security (FHS) features are supported for IPv6 on the Catalyst 4500-E and -X series switch:

- IPv6 RA Guard
- IPv6 Source Guard and Prefix Guard
- IPv6 Snooping
- DHCPv6 Guard
- IPv6 Neighbor Discovery Multicast Suppress

- IPv6 Destination Guard
- IPv6 RFCs

You can find information about these features at this location:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-e/ip6f-15-e-book.html

QoS

The following QoS features are supported for IPv6 on the Catalyst 4500 series switch:

- MQC packet classification
- MQC traffic shaping
- MQC traffic policing
- MQC packing marking and remarking
- Queueing

You can find information about these features at this location:

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

Management

The following management features are supported for IPv6 on the Catalyst 4500 series switch:

- Ping
- Syslog
- Netconf support
- SNMP
- SOAP
- HTTP(s)

You can find information about these features at this location:

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

Multicast

Traditional IP communication allows a host to send packets to a single host (unicast transmission) or to all hosts (broadcast transmission). IPv6 multicast, allows a host to send a single data stream to a subset of all hosts (group transmission) simultaneously.

The following multicast features are supported for IPv6 on the Catalyst 4500 series switch:

- Multicast Listener Discovery (MLD) protocol, versions 1 and 2

  You can find information about IPv6 MLD Snooping at this location:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/53SG/configuration/mldsnoop.html
- PIM Sparse Mode (PIM-SM)

- PIM Source Specific Multicast (PIM-SSM)
- Scope boundaries
- MLD access group
- PIM embedded Rendezvous Point (RP) support
- Static multicast routing (mroute)
- Explicit tracking of receivers
- Bootstrap routers (BSR)
- MLD snooping

You can find information about these features at this location:

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

Static Routes

Networking devices forward packets using route information that is either manually configured or dynamically learned using a routing protocol. Static routes are manually configured and define an explicit path between two networking devices. Unlike a dynamic routing protocol, static routes are not automatically updated and must be manually reconfigured if the network topology changes. The benefits of using static routes include security and resource efficiency. Static routes use less bandwidth than dynamic routing protocols and no CPU cycles are used to calculate and communicate routes. The main disadvantage to using static routes is the lack of automatic reconfiguration if the network topology changes.

Static routes can be redistributed into dynamic routing protocols but routes generated by dynamic routing protocols cannot be redistributed into the static routing table. No algorithm exists to prevent the configuration of routing loops that use static routes.

Static routes are useful for smaller networks with only one path to an outside network and to provide security for a larger network for certain types of traffic or links to other networks that need more control. In general, most networks use dynamic routing protocols to communicate between networking devices but may have one or two static routes configured for special cases.

You can find more information regarding static routes at:

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

First-Hop Redundancy Protocols

IPv6 routing protocols ensure router-to-router resilience and failover. However, in situations in which the path between a host and the first-hop router fails, or the first-hop router itself fails, First-Hop Redundancy Protocols (FHRPs) ensure host-to-router resilience and failover.

The Hot Standby Router Protocol (HSRP) protects data traffic in case of a gateway failure.

You can find more information about First-Hop Redundancy Protocols at:

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

Unicast Routing

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

RIP

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.

You can find more about RIP at this location:

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

OSPF

The switch running the IP services feature set supports Open Shortest Path First (OSPF) for IPv6, a link-state protocol for IP.

You can find more information about OSPF at this location:

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

EIGRP

The switch running the IP-services feature set 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.

You can find more information about EIGRP at this location:

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

IS-IS

Intermediate System-to-Intermediate System (IS-IS) 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.

You can find more information about Is-IS at this location:

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

Multiprotocol BGP

Multiprotocol Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP) used mainly to connect separate routing domains that contain independent routing policies (autonomous systems). Connecting to a service provider for access to the Internet is a common use for BGP. BGP can also be used within an autonomous system, which is referred to as internal BGP (iBGP). Multiprotocol BGP is an enhanced BGP that carries routing information for multiple network layer protocol address families, for example, IPv6 address family and for IP multicast routes. All BGP commands and routing policy capabilities can be used with multiprotocol BGP.

You can find more information about multiprotocol BGP at this location:

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

Tunneling

The following tunneling features are supported for IPv6 on the Catalyst 4500 series switch:

- Automatic 6to4
- ISATAP
- Configured tunnels

Note Tunneling is not supported in hardware but is supported in software.

You can find information about these features at this location:

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

IPv6 Default States

Table 57-1 shows the default states of IPv6 configuration.

Table 57-1 Default IPv6 Configuration

Feature	Default Setting
IPv6 routing	Disabled globally and on all interfaces
CEFv6 or dCEFv6	Disabled (IPv4 CEF and dCEF are enabled by default) **Note** When IPv6 routing is enabled, CEFv6 and dCEF6 are automatically enabled.
IPv6 addresses	None configured