CHAPTER 2

Overview of IPv6

Note The information in this chapter applies to both the ACE module and the ACE appliance unless otherwise noted.

This chapter describes Internet Protocol Version 6 (IPv6), why it is needed, and how it works. It includes the following major sections:

- Introduction to IPv6
- Methods of Transitioning from IPv4 to IPv6
- IPv6 Header Format
- IPv6 Addressing
- IPv6 Protocols and Support

Introduction to IPv6

This section describes IPv6, including a brief history of the protocol, why it is needed now, and some of the advantages of using it. The section contains the following subsections:

- What is IPv6?
- Why is IPv6 Needed Now?
- Advantages of IPv6

What is IPv6?

IPv6 is the replacement Internet protocol for IPv4. It corrects some of the deficiencies of IPv4 and simplifies the way that addresses are configured and how they are handled by Internet hosts.

IPv4 has proven to be robust, easily implemented, and interoperable, and has stood the test of scaling an internetwork to a global utility the size of the Internet. However, the initial design did not anticipate the following conditions:

- Recent exponential growth of the Internet and the impending exhaustion of the IPv4 address space
- The ability of Internet backbone routers to maintain large routing tables
- Need for simpler autoconfiguration and renumbering
- Requirement for security at the IP level (IPSec)
- Need for better support for real-time delivery of data, known as quality of service (QoS)

Why is IPv6 Needed Now?

With its 32-bit address format, IPv4 can handle a maximum 4.3 billion unique IP addresses. While this number may seem very large, it is not enough to sustain and scale the rapidly rising growth of the Internet. Although improvements to IPv4, including the use of NAT, have allowed the extended use of the protocol, address exhaustion is inevitable and could happen as soon as 2012.

With its 128-bit address format, IPv6 can support 3.4×10^{38} or 340,282,366,920,938,463,463,374,607,431,768,211,456 unique IP addresses. This number of addresses is large enough to configure a unique address on every node in the Internet and still have plenty of addresses left over. It is also large enough to eliminate the need for NAT, which has its own inherent problems.

A few countries, governmental agencies, and multinational corporations have either already deployed or mandated deployment of IPv6 in their networks and software products. Some emerging nations have no choice but to deploy IPv6 because of the unavailability of new IPv4 addresses.

Advantages of IPv6

Besides providing an almost limitless number of unique IP addresses for global end-to-end reachability and scalability, IPv6 has the following additional advantages:

- Simplified header format for efficient packet handling
- Larger payload for increased throughput and transport efficiency
- Hierarchical network architecture for routing efficiency
- Support for widely deployed routing protocols (OSPF, BGP, etc.)
- Autoconfiguration and plug-and-play support
- Elimination of need for network address translation (NAT) and application layered gateway (ALG)
- Increased number of multicast addresses

Methods of Transitioning from IPv4 to IPv6

The transition from IPv4 to IPv6 will not happen quickly because of the scope of the change. The two protocols will likely need to coexist for many years before IPv6 replaces IPv4 completely. Many countries and corporations are currently using one or more of the methods described below to transition their networks to IPv6.

Dual Stack

A dual stack means that IPv4 and IPv6 addresses coexist on the same platform and support hosts of both types. This method is a way to transition from IPv4 to IPv6 with coexistence as a first step. The ACE supports a dual stack arrangement for IPv6.

VPN Tunneling

The ACE does not support tunneling for IPv6.

NAT

The ACE acts as a proxy device by terminating connections from clients and then establishing a back-end connection with servers. It then splices the two connections together to allow the clients and servers to communicate with each other.

For IPv6, the ACE supports the NATing of client or VIP IPv4 addresses to server IPv6 and the reverse for HTTP and HTTPS load balancing.

IPv6 Header Format

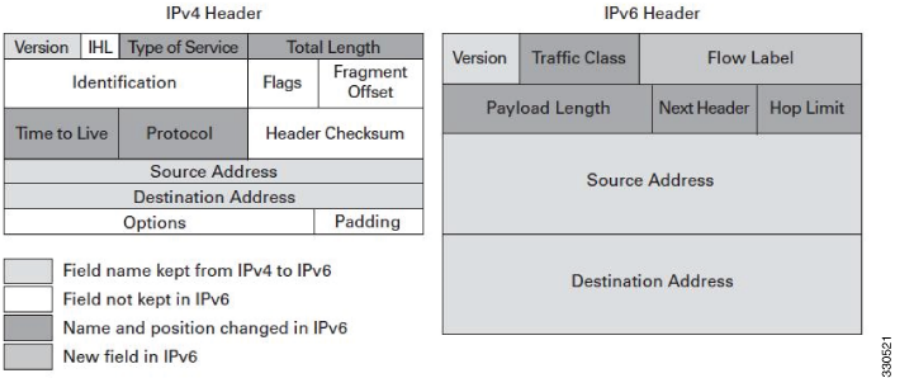
This section describes the IPv6 header format and how it differs from the IPv4 header format. It contains the following sections:

- IPv6 Header Format
- IPv6 Header Fields

IPv6 Header Format

A side-by-side comparison of the IPv4 header and the IPv6 header (Figure 2-1) shows that the IPv6 header is more streamlined and efficient than the IPv4 header.

Figure 2-1 IPv6 Header Format



IPv6 Header Fields

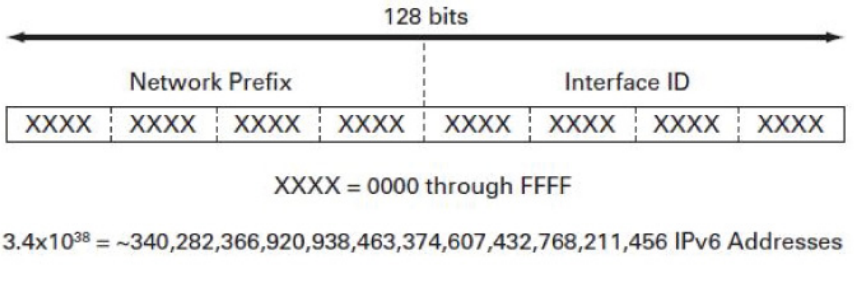
The IPv6 header contains the following fields:

- Version
- Traffic Class
- Flow Label
- Payload Length
- Next Header
- Hop Limit
- Source Address
- Destination Address

IPv6 Addressing

IPv6 addresses are 128 bits long. They are logically divided into a network prefix and a host identifier. The number of bits in the network prefix is represented by a prefix length (for example, /64). The remaining bits are used for the host identifier. If you do not specify a prefix length for an IPv6 address, the default prefix length is /64. See Figure 2-2.

Figure 2-2 IPv6 Address Format



Each IPv6 address type has a scope that describes the part of the network where the address is unique. Some IPv6 addresses are unique only in a subnet or a local network (link-local scope), others are unique in private networks or between organizations (unique-local scope), while still others are globally unique (global scope), that is, everywhere in the Internet.

Note that there is no concept of broadcast addresses in IPv6. For one to many addressing, use multicast addresses.

The ACE supports the compressed IPv6 address format where leading zeros in a 16-bit block are not shown and the longest string of 16-bit address blocks is compressed. All IPv6 addresses will display as compressed, but the CLI accepts both compressed and uncompressed addresses. For example, the following two addresses are equivalent:

```
2001:0000:ABCD:EF22:0000:1234:5678:0001
2001::ABCD:EF22:0:1234:5678:1
```

The double colon (::) in the second address indicates that a string of zeros has been omitted. You can use this compressed format only once in an address. If there are multiple contiguous strings of zeros in an address, you can replace them all with a double colon (::). Leading zeros can also be omitted, but not trailing zeros.

IPv6 supports the following types of addresses:

- Unicast Addresses
- Multicast Addresses

Unicast Addresses

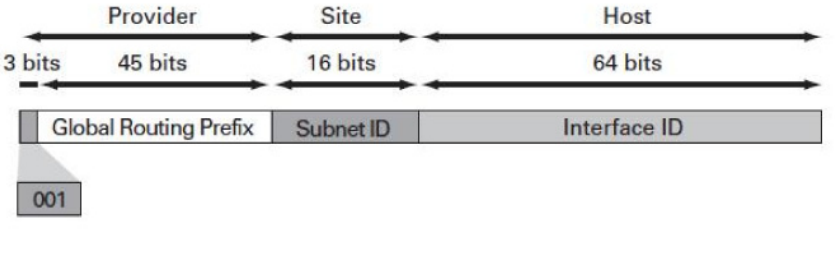
Use unicast for one-to-one communication between hosts. Unicast addresses work similarly for both IPv4 and IPv6. IPv6 supports several types of unicast addresses as described in the following sections.

- Global
- Link-Local
- Unique-Local
- Anycast Addresses

Global

A global IPv6 address is a unicast address with a predefined prefix of 2000::/3 (001). Cisco supports global IPv6 addresses in the range of 2000::/3 through 3000::/3. IPv6 addresses with a prefix of 2000::/3 (001) through E000::/3 (111), excluding the FF00::/8 (1111 1111) multicast addresses, are required to have 64-bit interface identifiers (VLAN IDs) in the IEEE 64-bit Extended Universal Identifier (EUI-64) format. The Internet Assigned Numbers Authority (IANA) allocates the IPv6 address space in the range of 2001::/16 to the registries. See Figure 2-3.

Figure 2-3 Global IPv6 Address Format



A global unicast address typically consists of a 48-bit global routing prefix and a 16-bit subnet ID. In the IPv6 aggregatable global unicast address format document (RFC 2374), the global routing prefix included two other hierarchically structured fields called Top-Level Aggregator and Next-Level Aggregator. Because these fields were policy-based, the IETF decided to remove the fields from the RFCs. However, some existing IPv6 networks deployed in the early days might still be using networks based on the older architecture.

A 16-bit subnet field called the Subnet ID can be used by individual organizations to create their own local addressing hierarchy and to identify subnets. This field allows an organization to use up to 65,535 individual subnets.

The IEEE 64-bit Extended Unique Identifier (EUI-64) is a global aggregatable address format that is used for generic IPv6 communication. All global addresses are required to include a 64-bit interface ID (VLAN ID) in the lowest 64 bits of the address. The lowest 64 bits of a global address can be assigned in one of several ways:

- Autoconfigured from EUI-64
- Expanded from a 48-bit MAC address (for example, an Ethernet address)
- Autogenerated pseudo-random number to address privacy concerns
- Assigned using DHCPv6
- Manually configured

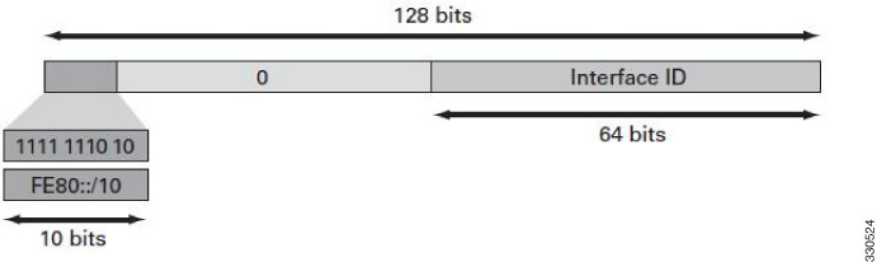
The EUI-64 format is used to perform stateless autoconfiguration. This format expands the 48-bit MAC address to 64 bits by inserting FFFE into the middle 16 bits between the upper three bytes (OUI field) and the lower 3 bytes (serial

number) of the link layer address. To better support the compression of addresses with a local scope, the seventh bit in the high-order byte of the MAC address (the universal/local “u” bit) is inverted.

Link-Local

A link-local address is a unicast address that has a scope of the local link only and one is required on every interface for IPv6 to work. The ACE automatically creates a link-local address for each IPv6-enabled interface using the EUI-64 format. Alternatively, the ACE accepts a user-configured link-local address. Each link-local address has a predefined prefix of FE80::/64. See Figure 2-4.

Figure 2-4 Link-Local Address Format



Link-local addresses have the following characteristics:

- Automatically assigned when you enable IPv6 using the **ipv6 enable** command
- Used for next-hop calculations in routing protocols
- The first ten bits of the prefix are always 1111 1110 10 (FE80::/64)
- The last 54 bits of the prefix can be zero or any configured value

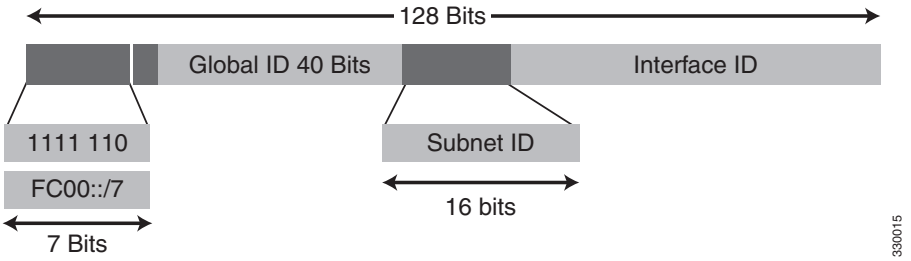
Unique-Local

A unique-local address is a unicast address that is valid only within a site or organization or between a limited number of sites. It is used for local communications and intersite VPNs. Unique-local addresses are similar to IPv4 private addresses and are not routable on the internet.

The first seven bits of the prefix are predefined as 1111 110 (FC00::/7). FC00::/7 is divided into two /8 blocks: FC00::/8 (eighth most significant bit set to 0) and FD00::/8 (eighth MSB set to 1). FC00::/8 is not defined yet. FD00::/8 is used with /48 prefixes by setting the 40 least significant bits (LSBs) to a randomly generated bit string. See Figure 2-5.

The ACE supports the EUI-64 format for both global and unique-local addresses. This format expands the 48-bit MAC address to 64 bits by inserting FFFE into the middle 16 bits between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To better support the compression of addresses with a local scope, the seventh bit in the high-order byte of the MAC address (the universal/local "u" bit) is inverted.

Figure 2-5 Unique-Local Address Format



Anycast Addresses

The ACE does not support anycast addressing for IPv6. Therefore, you cannot configure a single unicast address on multiple interfaces. If you attempt to do this, you will receive an error message.

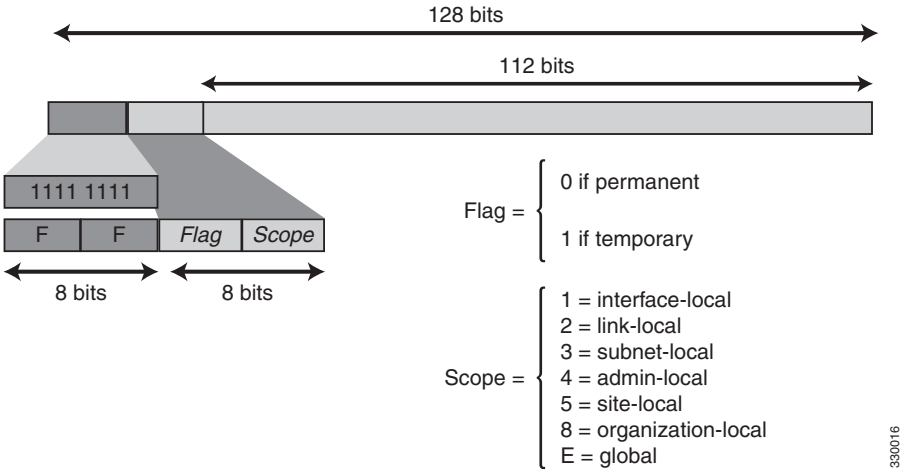
Multicast Addresses

An IPv6 multicast address has a predefined prefix of FF00::/8 (1111 1111). See Figure 2-6. The multicast address range uses 1/256 of the total IPv6 address space. An IPv6 multicast address is an identifier for a set of interfaces that typically belong to different nodes.

The ACE does not support the configuration of multicast addresses on interfaces. It does receive and process packets for the following addresses:

- All-nodes multicast group (FF02::1)
- Solicited node multicast group (FF02::1:ff00:0000/104)
- All-router multicast group (FF02::2)

Figure 2-6 Multicast Address Format



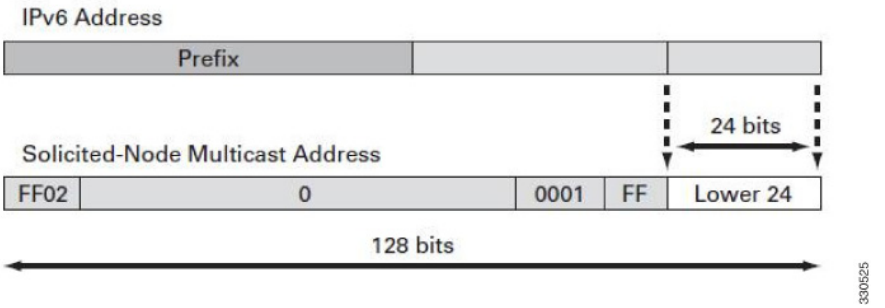
The second octet following the predefined prefix defines the lifetime and scope of the multicast address. A permanent (well-known) multicast address has a lifetime parameter equal to 0 and is assigned by IANA. A temporary multicast address has a lifetime parameter equal to 1 and is dynamically assigned. A multicast address that has the scope of an interface, link, subnet, admin, site, organization, or a global scope has a scope parameter of 1, 2, 3, 4, 5, 8, or E, respectively. The IPv6 addressing scheme is designed to support millions of multicast group addresses.

Solicited-Node Multicast Address

An IPv6 solicited-node address is used to send messages in the neighbor discovery (ND) protocol. ND is the IPv6 equivalent of ARP. For more information about ND, see Chapter 6, Configuring Neighbor Discovery.

A solicited-node multicast address is a multicast group address that corresponds to an IPv6 unicast address. An IPv6 node must join the associated solicited-node multicast group for every unicast address it has been assigned. A solicited-node multicast address has the prefix FF02:0:0:0:0:1:FF00:0000/104 concatenated with the 24 low-order bits of a corresponding IPv6 unicast or anycast address, as shown in Figure 2-7.

Figure 2-7 Solicited Node Multicast Address Format



For example, the solicited-node multicast address corresponding to the IPv6 global unicast address 2001::01:800:200E:8C6C is FF02::1:FF0E:8C6C.

IPv6 Protocols and Support

The ACE supports the following IPv6 protocols that are described in the following sections:

- Neighbor Discovery
- Router Discovery
- Duplicate Address Detection
- ICMPv6
- DHCPv6

Neighbor Discovery

Neighbor discovery (ND) is the protocol that the ACE uses to find other nodes on the same subnet. ND is always enabled when the interface is IPv6 enabled. A management policy on the interface is not necessary for ND to function on the interface. It will also not be possible to disable ND on the interface by configuring any kind of policy.

The ACE sends neighbor solicitation (NS) messages to resolve addresses, for neighbor unreachability detection (NUD), and duplicate address detection (DAD).

The ACE sends out both solicited and unsolicited neighbor advertisements (NAs). It responds to an NS when the target address of the NS is either configured on an enabled IPv6 interface or is configured as a VIP or NAT address on the interface.

The ACE supports statically defined neighbor link-local to Layer 2 address mappings on an interface. These mappings are not timed out or overwritten by the ND process and they can be removed only through configuration. If the address already exists in the cache at the time of configuration, the cached entry is overwritten by the configured one and becomes static.

Router Discovery

Router discovery (RD) is the process that the ACE uses to advertise its presence on the local subnet. The ACE sends out both solicited and unsolicited router advertisements (RAs). Although the ACE does not send out router solicitation (RS) messages, it does to respond to RS messages from its neighbors.

Duplicate Address Detection

duplicate address detection (DAD) is an IPv6 mechanism that detects duplicate addresses in a subnet. If a duplicate address is found on an interface, the duplicate address is disabled on the originating interface until the problem is resolved. If the link-local address is a duplicate, then all addresses on the IPv6 interface are disabled until the address problem is resolved.

ICMPv6

The ACE supports ICMPv6 management policies and ICMPv6 ACLs.

The ACE does not send out ICMPv6 redirects because the ACE does not support dynamic routing protocols and should not advise hosts about what is the best route.

DHCPv6

DHCP relay is an agent that resides between clients and DHCP servers, and forwards client requests to servers and server replies back to clients. For IPv6, DHCP is the stateful address autoconfiguration protocol, from which the clients can receive addressing information from DHCP servers. The ACE supports DHCPv6 relay only.

Clients can also query the DHCP servers for other configuration information (for example, DNS and NTP (appliance only) servers).

To identify the client interface to which a server reply must be forwarded, the ACE uses the interface ID (VLAN ID) DHCP option. The ACE will add this option to the Relay-Forward messages that it generates from the client request. The option value is the interface ID (VLAN ID) of the interface on which the client request is received. The server replies in a Relay-Reply message with this option value intact. The ACE knows which interface to use to send the reply on by reading back this option from the Relay-Reply message.

The DHCPv6 relay process configures ACLs so that it receives all the relevant DHCPv6 packets, and then processes the packets and sends them out according to the user configuration.