Next Generation IP

IPv6 ADDRESSING

- The main reason for migration from IPv4 to IPv6 is the small size of the address space in IPv4.
- **Representation:**
- Several notations have been proposed to represent IPv6 addresses. The following shows two of these notations: binary and colon hexadecimal.

Binary: (128 bits) 1111111011110110 … 1111111100000000

Colon Hexadecimal: FEF6:BA98:7654:3210:ADEF:BBFF:2922:FF00

- **Abbreviation:**
- Although an IPv6 address, even in hexadecimal format, is very long, many of the digits are zeros. In this case, we can abbreviate the address. The leading zeros of a section can be omitted. Using this form of abbreviation, 0074 can be written as 74, 000F as F, and 0000 as 0.
- **FDEC:0:0:0:0:BBFF:0:FFFF FDEC::BBFF:0:FFFF**

Continue…

- **Mixed Notation:**
- Sometimes we see a mixed representation of an IPv6 address: colon hex and dotteddecimal notation. This is appropriate during the transition period in which an IPv4 address is embedded in an IPv6 address (as the rightmost 32 bits).
- However, this happens when all or most of the leftmost sections of the IPv6 address are 0s. For example, the address (::130.24.24.18) is a legitimate address in IPv6.
- **CIDR Notation:**
- IPv6 uses hierarchical addressing. For this reason, IPv6 allows slash or CIDR notation. For example, the following shows how we can define a prefix of 60 bits using CIDR.
- E.g. **FDEC::BBFF:0:FFFF/60**

Continue…

- **Address Space:**
- The address space of IPv6 contains 2^{128} addresses.
- **Three Address Types:**
  1) **Unicast Address:** A unicast address defines a single interface (computer or router). The packet sent to a unicast address will be routed to the intended recipient.
  2) **Anycast Address:** An anycast address defines a group of computers that all share a single address. A packet with an anycast address is delivered to only one member of the group, the most reachable one.
  3) **Multicast Address:** A multicast address also defines a group of computers. However, there is a difference between anycasting and multicasting. In anycasting, only one copy of the packet is sent to one of the members of the group; in multicasting each member of the group receives a copy.

Continue…

- **Address Space Allocation:**

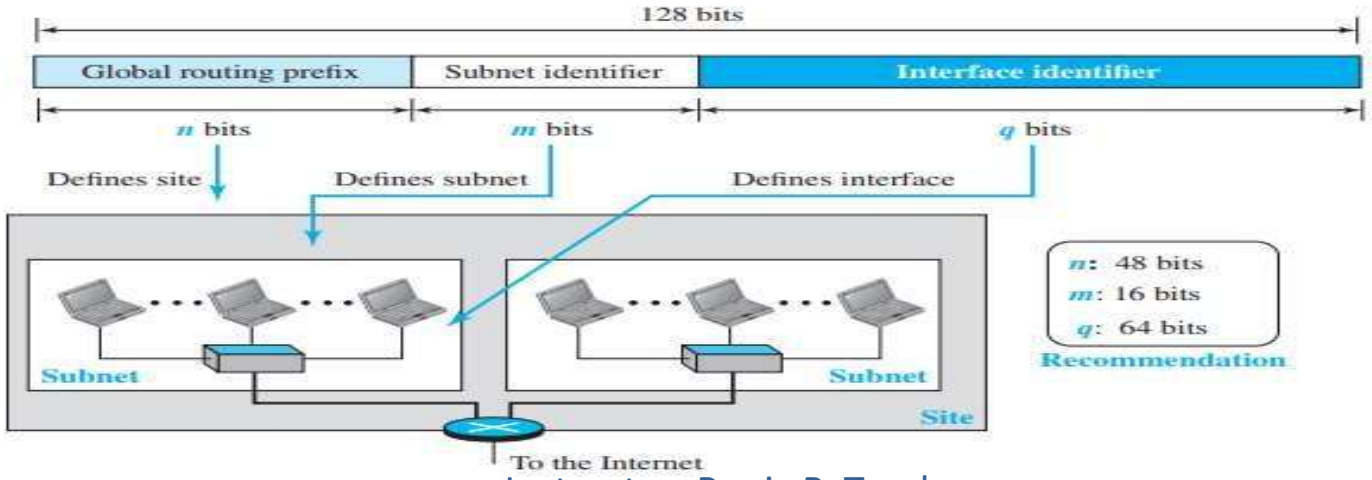
Table 22.1 *Prefixes for assigned IPv6 addresses*

Block prefix	*CIDR*	*Block assignment*	*Fraction*
0000 0000	0000::/8	Special addresses	1/256
001	2000::/3	Global unicast	1/8
1111 110	FC00::/7	Unique local unicast	1/128
1111 1110 10	FE80::/10	Link local addresses	1/1024
1111 1111	FF00::/8	Multicast addresses	1/256

Continue…

- **Global Unicast Addresses:**
- The block in the address space that is used for unicast (one-to-one) communication between two hosts in the Internet is called the global unicast address block. CIDR for the block is 2000::/3, which means that the three leftmost bits are the same for all addresses in this block (001). The size of this block is 2^{125} bits, which is more than enough.
- An address in this block is divided into three parts**: global routing prefix (n bits)**, **subnet identifier (m bits)**, and **interface identifier (q bits)**

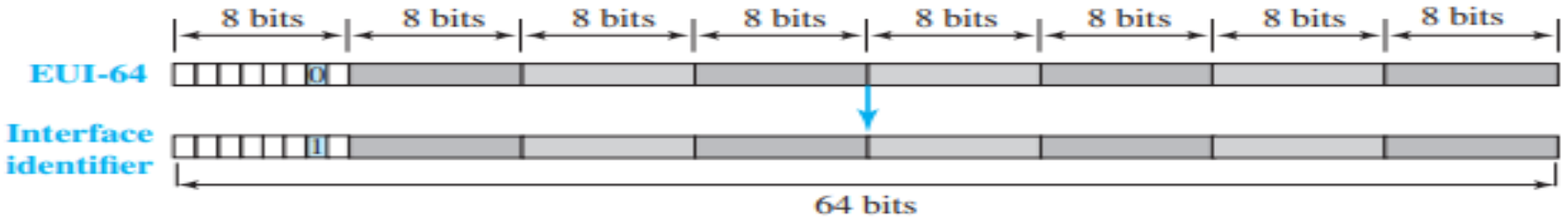
Figure 22.1 *Global unicast address*



Continue…

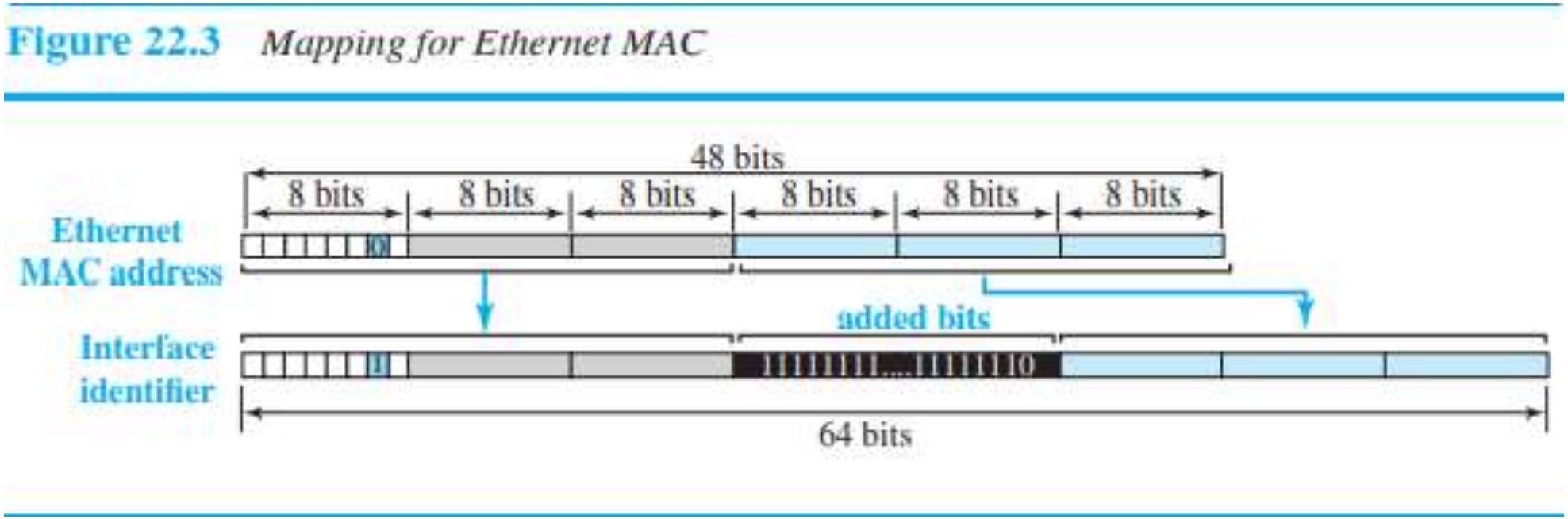
- In IPv4 addressing, there is not a specific relation between the hostid (at the IP level) and link-layer address (at the data-link layer) because the link-layer address is normally much longer than the hostid.
- The IPv6 addressing allows this relationship. A link-layer address whose length is less than 64 bits can be embedded as the whole or part of the interface identifier, eliminating the mapping process. Two common link-layer addressing schemes can be considered for this purpose: the **64-bit extended unique identifier (EUI-64)** defined by IEEE and the **48-bit link-layer address** defined by Ethernet.
- **Mapping EUI-64:** To map a 64-bit physical address, the global/local bit of this format needs to be changed from 0 to 1 (local to global) to define an interface address.

Figure 22.2 *Mapping for EUI-64*



Continue…

- **Mapping Ethernet MAC Address:**
- We need to change the local/global bit to 1 and insert an additional 16 bits. The additional 16 bits are defined as 15 ones followed by one zero, or FFFE16.



THE IPv6 PROTOCOL

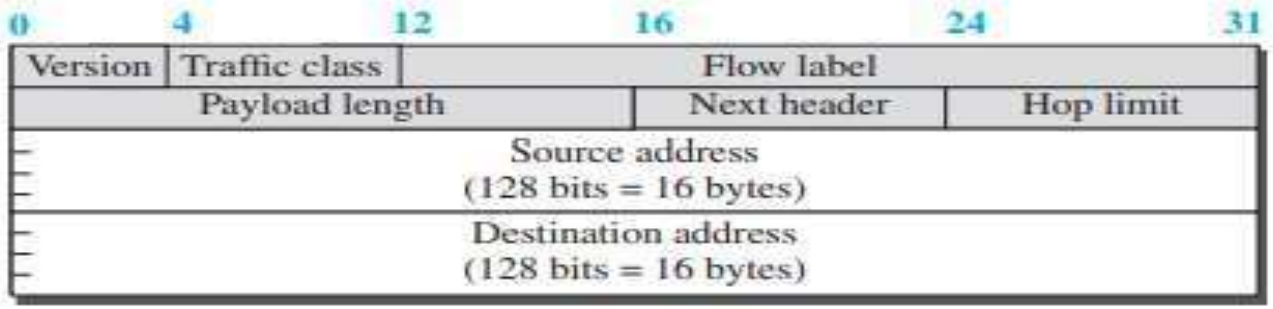
- The following shows other changes implemented in the protocol in addition to changing address size and format.
- **Better header format.** IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.
- **New options.** IPv6 has new options to allow for additional functionalities.
- **Allowance for extension.** IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.
- **Support for resource allocation.** In IPv6, the type-of-service field has been removed, but two new fields, traffic class and flow label, have been added to enable the source to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video.
- **Support for more security.** The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

Packet Format

- Each packet is composed of a base header followed by the payload. The base header occupies 40 bytes, whereas payload can be up to 65,535 bytes of information.

Figure 22.6 *IPv6 datagram*

a. IPv6 packet



b. Base header

Continue…

- **Version.** The 4-bit version field defines the version number of the IP.
- **Traffic class.** The 8-bit traffic class field is used to distinguish different payloads with different delivery requirements.
- **Flow label.** The flow label is a 20-bit field that is designed to provide special handling for a particular flow of data.
- **Payload length.** The 2-byte payload length field defines the length of the IP datagram excluding the header.
- **Next header.** The next header is an 8-bit field defining the type of the first extension header (if present) or the type of the data that follows the base header in the datagram.
- **Hop limit.** The 8-bit hop limit field serves the same purpose as the TTL field in IPv4.
- **Source and destination addresses.** A each 16-byte (128-bit) Internet address that identifies the original source and destination address of the datagram respectively .
- **Payload.** The payload in IPv6 means a combination of zero or more extension headers (options) followed by the data from other protocols (UDP, TCP, and so on).

Continue…

- **Extension Header:**
- An IPv6 packet is made of a base header and some extension headers. The length of the base header is fixed at 40 bytes. However, to give more functionality to the IP datagram, the base header can be followed by up to six extension headers.
- Six types of extension headers have been defined. These are hop-by-hop option, source routing, fragmentation, authentication, encrypted security payload, and destination option.
- **Hop-by-Hop Option** The hop-by-hop option is used when the source needs to pass information to all routers visited by the datagram.
- **Destination Option** The destination option is used when the source needs to pass information to the destination only.
- **Source Routing** The source routing extension header combines the concepts of the strict source route and the loose source route options of IPv4.

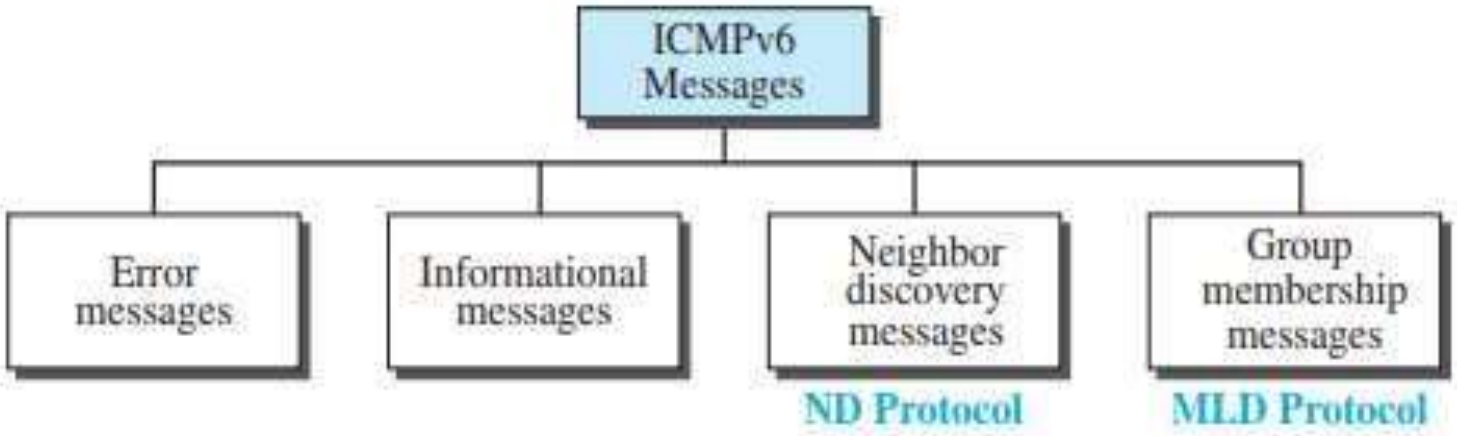
Continue…

- **Fragmentation** In IPv6, only the original source can fragment. A source must use a Path MTU Discovery technique to find the smallest MTU supported by any network on the path. The source then fragments using this knowledge.
- **Authentication** The authentication extension header has a dual purpose: it validates the message sender and ensures the integrity of data.
- **Encrypted Security Payload** The encrypted security payload (ESP) is an extension that provides confidentiality and guards against eavesdropping.

THE ICMPv6 PROTOCOL

- Another protocol that has been modified in version 6 of the TCP/IP protocol suite is **ICMP.**
- The ICMP, ARP and IGMP protocols in version are combined into one single protocol, ICMPv6.

Figure 22.10 *Categories of ICMPv6 messages*



Continue…

- **Error-Reporting Messages:**
- Four types of errors are handled: destination unreachable, packet too big, time exceeded, and parameter problems.
- **Informational Messages:**
- Two of the ICMPv6 messages can be categorized as informational messages: echo request and echo reply messages.
- **Neighbor-Discovery Messages:**

1) **Router-Solicitation Message** A host uses the router-solicitation message to find a router in the network that can forward an IPv6 datagram for the host.
2) **Router-Advertisement Message** The router-advertisement message is sent by a router in response to a router solicitation message.
3) **Neighbor-Solicitation Message** The neighbor solicitation message has the same duty as the ARP request message. This message is sent when a host or router has a message to send to a neighbor. The sender knows the IP address of the receiver, but needs the data-link address of the receiver.

Continue…

4) **Neighbor-Advertisement Message** The neighbor-advertisement message is sent in response to the neighbor-solicitation message.
5) **Redirection Message** The purpose of the redirection message is the same as described for version 4.
6) **Inverse-Neighbor-Solicitation Message** The inverse-neighbor-solicitation message is sent by a node that knows the link-layer address of a neighbor, but not the neighbor's IP address.
7) **Inverse-Neighbor-Advertisement Message** The inverse-neighbor-advertisement message is sent in response to the inverse-neighbor-discovery message.

- **Group Membership Messages:**
- The management of multicast delivery handling in IPv6 is given to the **Multicast Listener Delivery** protocol.
- MLDv2 has two types of messages: membership-query message and membership-report message.

Continue…

1) **Membership-Query Message** A membership-query message is sent by a router to find active group members in the network.
2) **Membership-Report Message** The format of the membership report in MLDv2 is exactly the same as the one in IGMPv3 except that the sizes of the fields are changed because of the address size