SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

Department of Information Technology

Course Name – 19IT401 Computer Networks

II Year / IV Semester

Unit 3 – Network Layer

Topic 4- IPv6

IPv6

- The main reason for migration from IPv4 to IPv6 is the small size of the address space in IPv4..
  - high-density mobility,
  - strong security.

- An IPv6 address is 128 bits or 16 bytes (octets) long, four times the address length in IPv4.

Address Representation (Address notations)
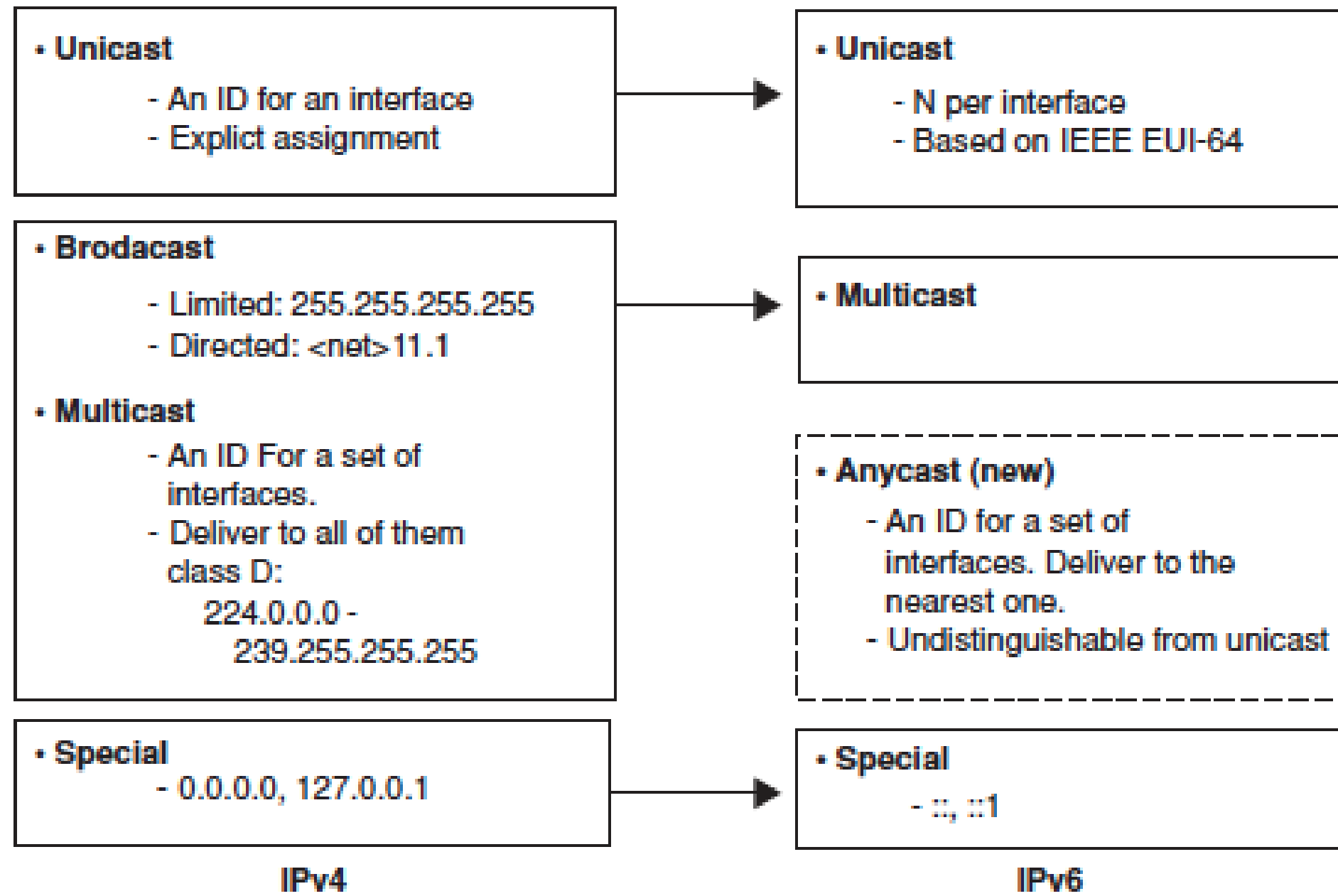The following shows two of these notations:
- binary and
- colon hexadecimal

Binary (128 bits)	1111111011110110 ... 1111111100000000
Colon Hexadecimal	FEF6:BA98:7654:3210:ADEF:BBFF:2922:FF00

IP Version	Size of Address Space
IPv6	128 bits, which allows for 2^{128} or 340,282,366,920,938,463,463,374,607,431,768,211,456 (3.4×10^{38}) possible addresses
IPv4	32 bits, which allows for 2^{32} or 4,294,967,296 possible addresses

IPv6

Address Types


```
• Unicast
    - An ID for an interface
    - Explict assignment

• Brodacast
    - Limited: 255.255.255.255
    - Directed: <net>11.1

• Multicast
    - An ID For a set of
      interfaces.
    - Deliver to all of them
      class D:
         224.0.0.0 -
         239.255.255.255

• Special
    - 0.0.0.0, 127.0.0.1

            IPv4
```

```
• Unicast
    - N per interface
    - Based on IEEE EUI-64

• Multicast

• Anycast (new)
    - An ID for a set of
      interfaces. Deliver to the
      nearest one.
    - Undistinguishable from unicast

• Special
    - ::, ::1

            IPv6
```

Changes in IPv6 Addressing

- Unicast - A unicast address defines a single interface.

- Multicast - A multicast address defines a group of computers. in multicasting each member of the group receives a copy

- Anycast – An anycast address defines a group of computers that all share a single address. Totally a new approach, "send to any one member of this specific group". only one copy will be sent.

IPv6

Address Types

Special Address
- **The unspecified address** is a subblock containing only one address, which is used during bootstrap when a host does not know its own address and wants to send an inquiry to find it.

- **The loopback address** also consists of one address. It is internal address that routes messages back to the local system. An address that sends outgoing signals back to the same computer for testing. The loopback address in IPv4 is 127.0.0.1. In IPv6, the loopback address is 0:0:0:0:0:0:0:1 or ::1.

- **A compatible address** is an address of 116 bits of zero followed by 32 bits of IPv4 address. It is used when a computer using IPv6 wants to send a message to another computer using IPv6.

- **A mapped address** is used when a computer already migrated to version 6 wants to send an address to a computer still using version 4.

IPv6

Special Feature of IPv6
Auto-configuration
In IPv6, DHCP protocol can still be used to allocate an IPv6 address to a host, but a host can also configure itself.
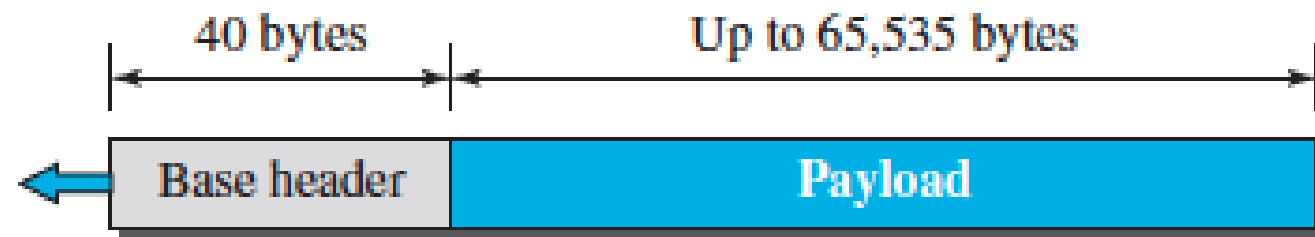
When a host in IPv6 joins a network, it can configure itself without the use of DHCP.
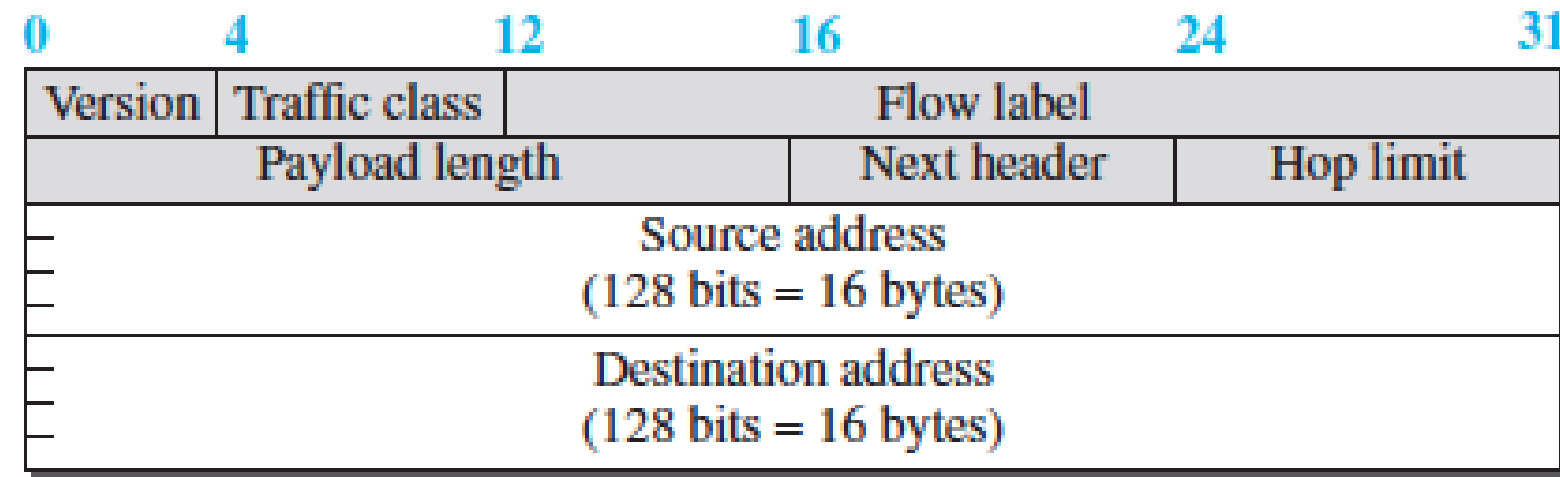
THE IPv6 PROTOCOL
• Better header format
• New options
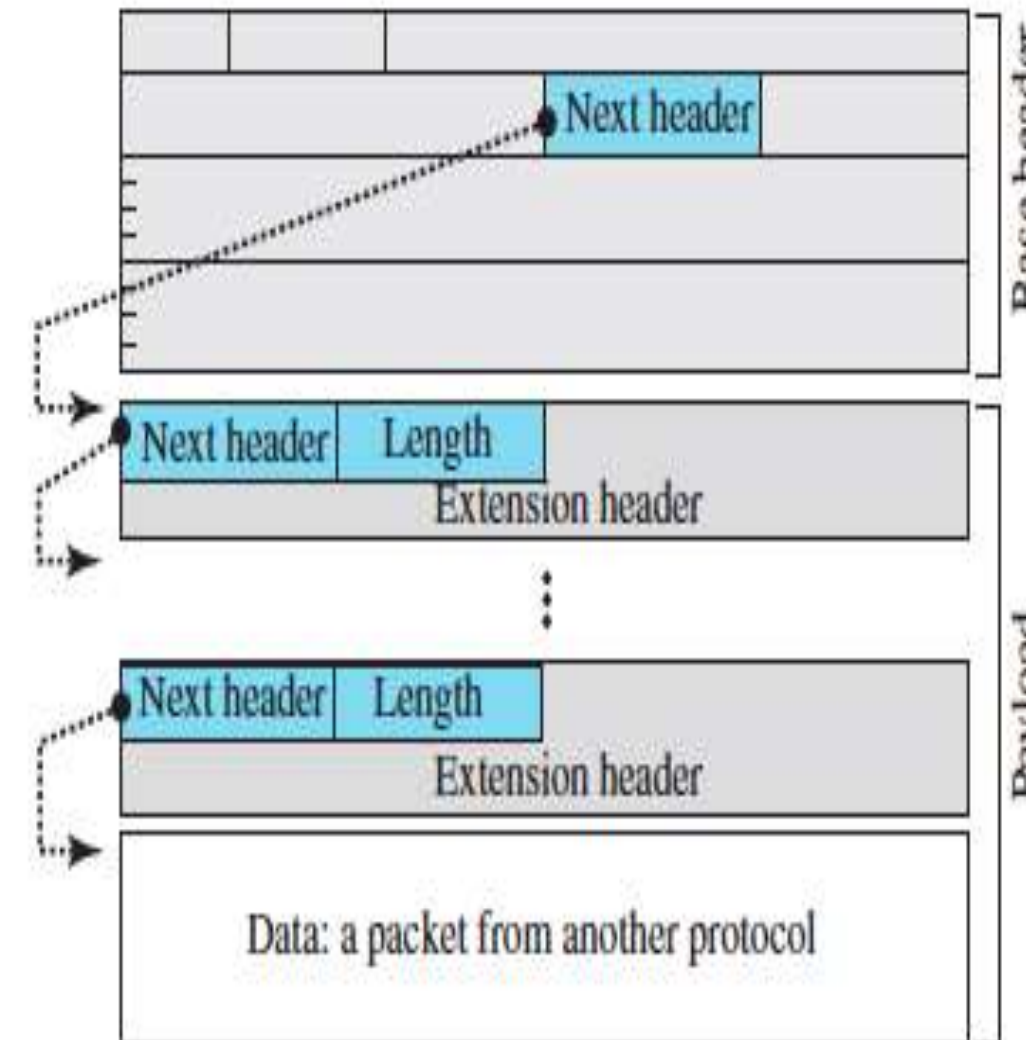• Allowance for extension
• Support for more security

IPv6

Packet Format

a. IPv6 packet

Version	Traffic class	Flow label		
Payload length			Next header	Hop limit
Source address (128 bits = 16 bytes)				
Destination address (128 bits = 16 bytes)				

b. Base header

Some next-header codes

00: Hop-by-hop option
02: ICMPv6
06: TCP
17: UDP
43: Source-routing option
44: Fragmentation option
50: Encrypted security payload
51: Authentication header
59: Null (no next header)
60: Destination option

IPv6

Every packet has **IPv6 header** and an **IPv6 payload**.

The IPv6 header consists of two parts, the **IPv6 base header** and optional **extension headers**

The header size is fixed 40 bytes.

**Version** - The 4-bit version field defines the version number of the IP. For IPv6, the value is 6.

Traffic class - The 8-bit traffic class field is used to distinguish different payloads with different delivery requirements. It replaces the type-of-service field in IPv4. Differentiated Services and Priority field used for Explicit congestion notification.

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.

IPv6
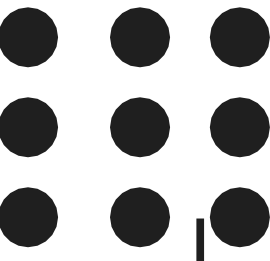
Next header - The next header is an 8-bit field defining the type of the first extension header (if present) or the type of the data that follows the base header in the datagram. Replaces protocol field in IPv4.

Hop limit - The 8-bit hop limit field serves the same purpose as the TTL field in IPv4.

Source and destination addresses - The source address field is a 16-byte (128-bit) Internet address that identifies the original source of the datagram. The destination address field is a 16-byte (128-bit) Internet address that identifies the destination of the datagram.

Payload - Compared to IPv4, the payload field in IPv6 has a different format and meaning
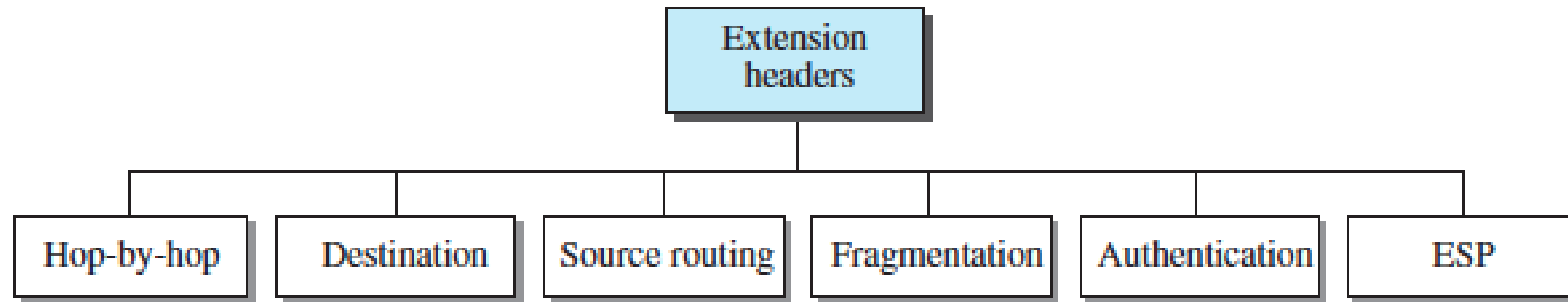
Extension Header

The length of the base header is fixed at 40 bytes. Six types of extension headers have been defined.

Hop-by-Hop Option – This option is used when the source needs to pass information to all routers visited by the datagram.

Destination Option – This option is used when the source needs to pass information to the destination only. Intermediate routers are not permitted access to this information.

Source Routing - The source routing extension header combines the concepts of the strict source route and the loose source route options of IPv4.
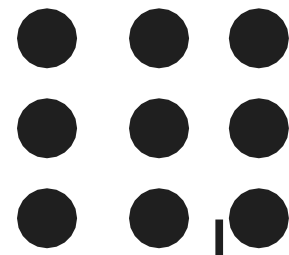
Extension Header

Fragmentation - The concept of fragmentation in IPv6 is the same as that in IPv4.

Authentication
- The authentication extension header has a dual purpose: it validates the message sender and ensures the integrity of data.

- Authentication is needed so the receiver can be sure that a message is from the genuine sender and not from an imposter.

- The integrity needed to check that the data is not altered in transition by some hacker.

Encrypted Security Payload
The encrypted security payload (ESP) is an extension that provides confidentiality and guards against eavesdropping. No one can view the contents of the message.

THANK YOU