SNS COLLEGE OF TECHNOLOGY

Coimbatore-35.
An Autonomous Institution

COURSE NAME : Internet of Things

III YEAR/ V SEMESTER

UNIT – IV IPv6 TECHNOLOGIES FOR THE IoT
Topic: ADDRESS CAPABILITIES

Dr.K.Sangeetha
HoD
Department of Computer Science and Engineering

IPv4 Addressing and Issues

- 2 ^32 addresses, based on a four-octet address space

- 32-bit (4-byte) binary address used to identify a host's network ID.

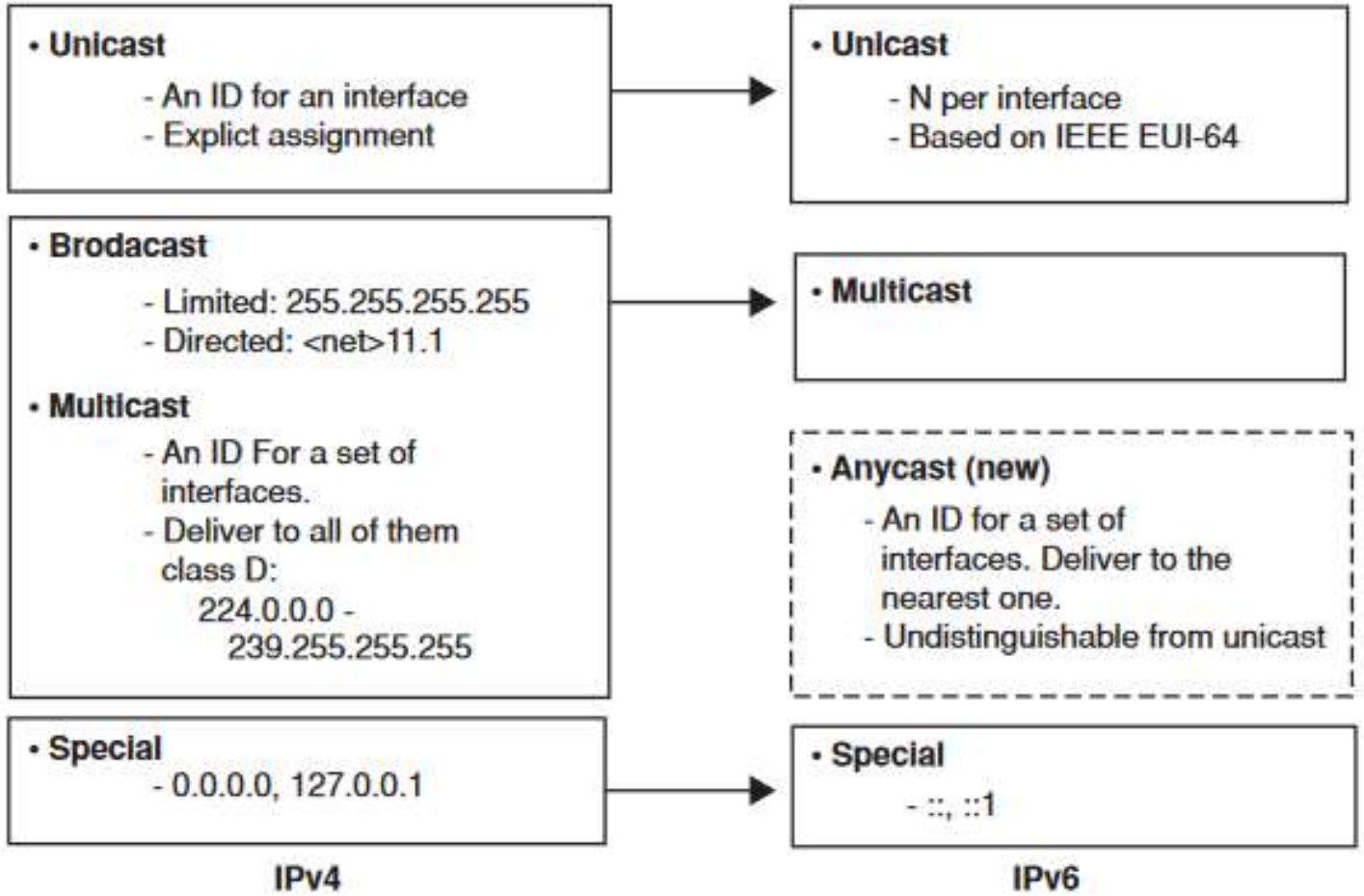
➢ It is represented by the nomenclature a.b.c.d (each of a, b, c, and d being from 1 to 255) (0 has a special meaning). Examples are 167.168.169.170, 232.233.229.209, and 200.100.200.100.

➢ **network address translation (NAT) mechanisms** are employed by organizations and even home users. This mechanism consists of using only a small set of public IPv4 addresses for an entire network to access the Internet.

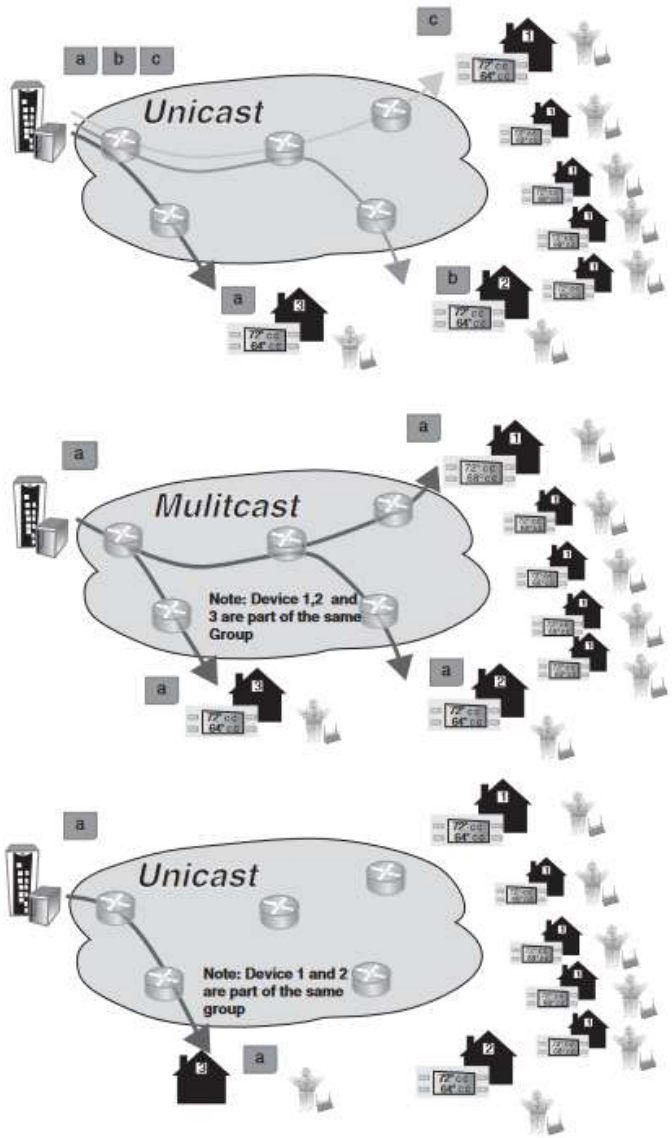
➢ Class A or Class C address that are locally unique but are duplicatively used and reused within various organizations

- Multimedia applications such as videoconferencing, VoIP, or video-on- demand/IPTV do not work smoothly through NAT devices. Multimedia applications make use of real-time transport protocol (RTP) and real-time control protocol (RTCP).
- These in turn use User Datagram Protocol (UDP) with dynamic allocation of ports and NAT does not directly
- IPsec is used extensively for data authentication, integrity, and confidentialityupport this environment
- Multicast,

IPv6 Address Space



- Unicast transmission: "send to this one specific address"
- Multicast transmission: "send to every member of this specific group"
- Anycast transmission: "send to any one member of this specific group." Typically (motivated by efficiency goals), the transmission occurs to the closest (in routing terms) member of the group. Generally one interprets anycast to mean "send to the closest member of this specific group."



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 PROTOCOL OVERVIEW

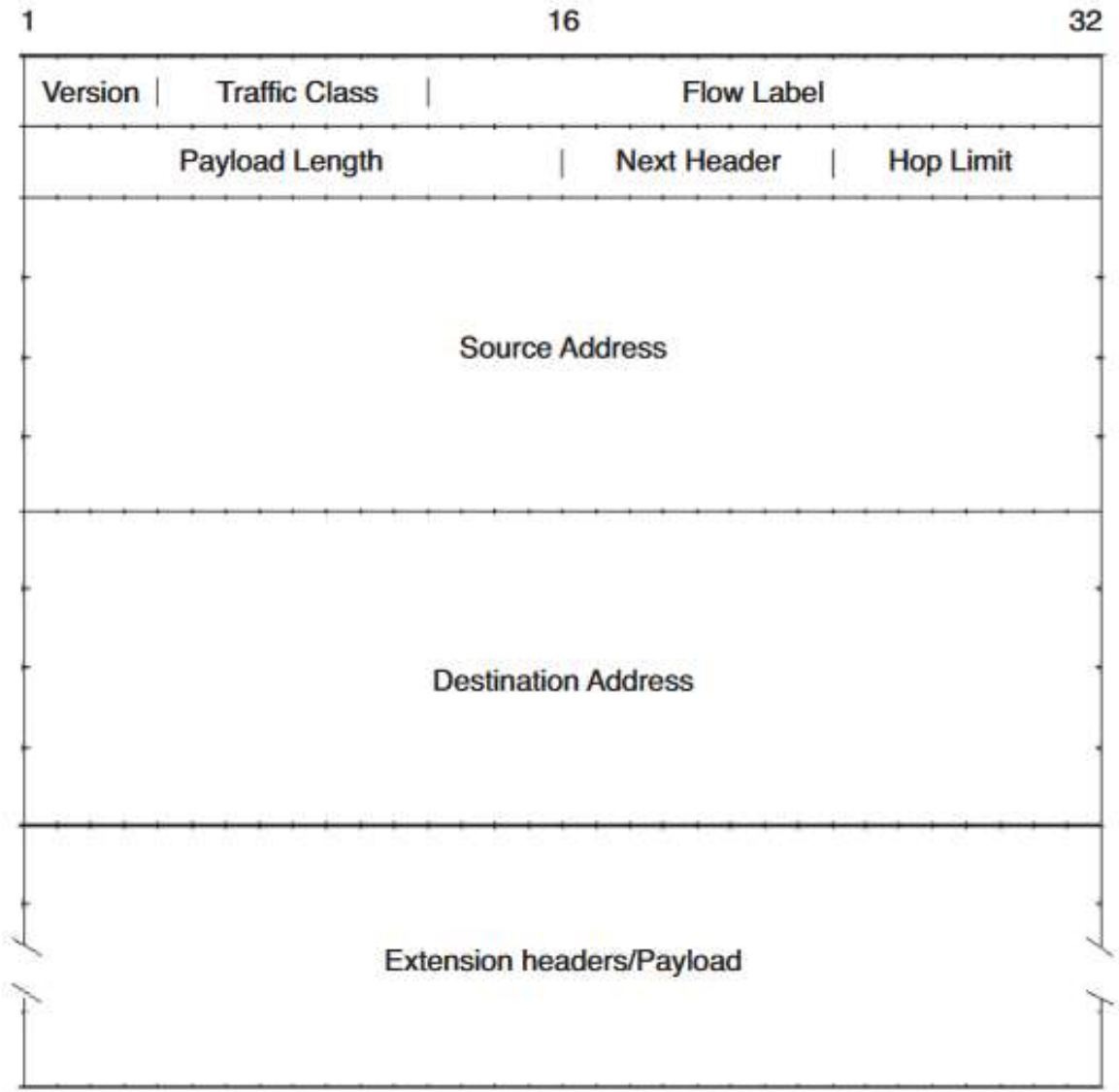
- ✓ Addressing
- ✓ Anycast
- ✓ Flow Labels
- ✓ ICMPv6
- ✓ Neighbor discovery

IPv6 is a connectionless datagram protocol used primarily for addressing and routing packets between hosts.

- ✓ Connectionless means that a session is not established before exchanging data
- ✓ Unreliable" means that delivery is not guaranteed

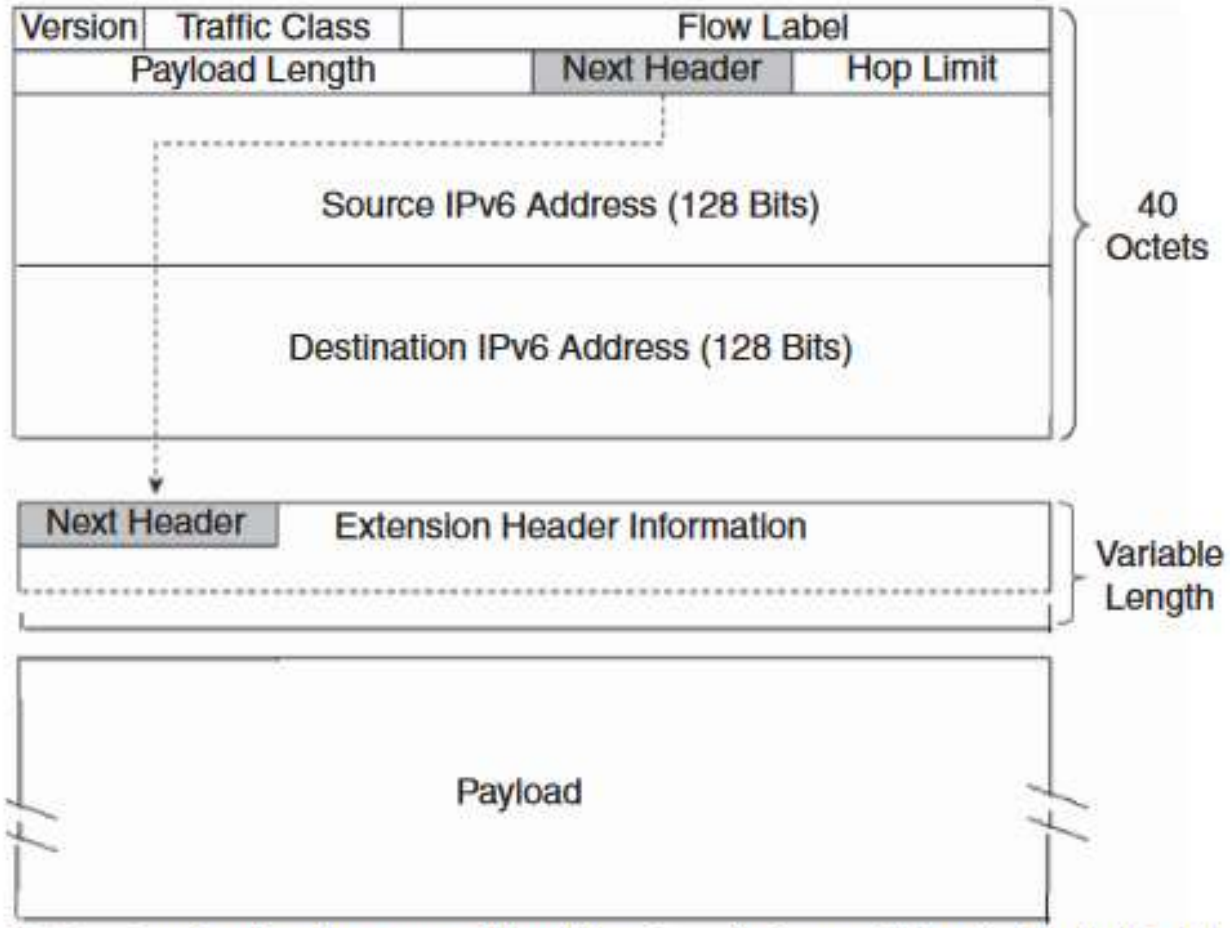
- ✓ IPv6 always makes a **best-effort attempt** to deliver a packet.
- ✓ An IPv6 packet might be lost, delivered out of sequence, duplicated, or delayed

IPV6 Packet



IPv6 datagram= IPv6 header + IPv6 payload

IPV6 extension header



IPv6 extension headers are optional headers that may follow the basic IPv6 header. An IPv6 PDU may include zero, one, or multiple extension headers. When multiple extension headers are used, they form a chained list of headers identified by the Next Header field of the previous header.

TABLE 7.4 IPv6 Base Header

IPv6 Header Field	Length (bits)	Function
Version	4	Identifies the version of the protocol. For IPv6, the version is 6
Traffic class	8	Intended for originating nodes and forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets
Flow label	20	(sometimes referred to as flow ID) Defines how traffic is handled and identified. A flow is a sequence of packets sent either to a unicast or to a multicast destination. This field identifies packets that require special handling by the IPv6 node. The following list shows the ways the field is handled if a host or router does not support flow label field functions: • If the packet is being sent, the field is set to zero • If the packet is being received, the field is ignored
Payload length	16	Identifies the length, in octets, of the payload. This field is a 16-bit unsigned integer. The payload includes the optional extension headers, as well as the upper-layer protocols, for example, TCP
Next header	8	Identifies the header immediately following the IPv6 header. The following shows examples of the next header: • 00 = Hop-by-hop options • 01 = ICMPv4 • 04 = IP in IP (encapsulation) • 06 = TCP • 17 = UDP • 43 = Routing • 44 = Fragment • 50 = Encapsulating security payload • 51 = Authentication • 58 = ICMPv6
Hop limit	8	Identifies the number of network segments, also known as links or subnets, on which the packet is allowed to travel before being discarded by a router. The hop limit is set by the sending host and is used to prevent packets from endlessly circulating on an IPv6 internetwork When forwarding an IPv6 packet, IPv6 routers must decrease the hop limit by 1 and must discard the IPv6 packet when the hop limit is 0
Source address	128	Identifies the IPv6 address of the original source of the IPv6 packet
Destination address	128	Identifies the IPv6 address of intermediate or final destination of the IPv6 packet


Thank You!