SNJB’s KBJ College of Engineering

Chandwad–423101 (Nashik)

Department
of
Information Technology

Subject : Internet of Things (IOT) of BE 2015 Pattern

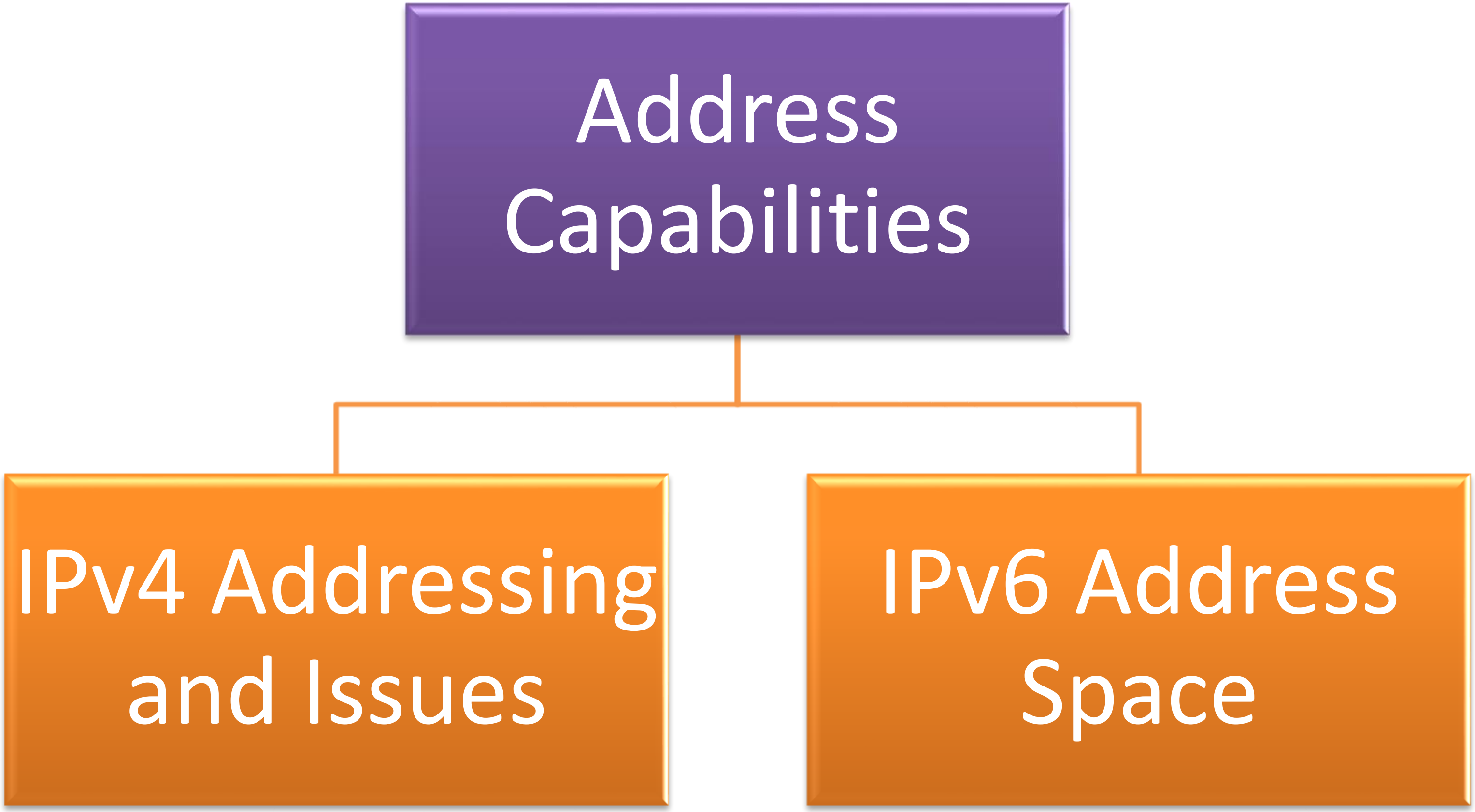
Unit 4
ADDRESSING TECHNIQUES FOR THE IoT

Overview and Motivations

- IPv6 is newer version of network layer protocol that is designed to coexist with IPv4
- IPv6 is expected to replace IPv4, but that will not happen overnight
- Current IPv4 has been in use for over 30 years
- IPv4 exhibits some challenges in supporting emerging demands for address space, high-density mobility, multimedia & strong security

Overview and Motivations

- IPv6 offers the potential of achieving
  - Scalability
  - Reachability
  - End-to-end Interworking
  - Quality of Service (QoS)
  - Commercial Grade Robustness
- Needed for current & emerging web services, data services, mobile video & IoT applications



Address Capabilities

IPv4 Addressing and Issues

IPv6 Address Space

IPv4 Addressing and Issues

- IPv4 theoretically allows up to 2^{32} addresses based on a four-octet address space
- So 429,49,67,296 unique values which can be considered as sequence of 256 “/8s,”
- Each “/8” corresponds to 16,777,216 unique address values
- Public, globally unique addresses are assigned by IANA (Internet assigned numbers authority)

IPv4 Addressing and Issues

- IP addresses are addresses of nodes; each device on network must have unique address
- In IPv4, it is 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)
- Examples are 167.168.169.170, 232.233.229.209, and 200.100.200.100

IPv4 Addressing and Issues

- Problem is that during 1980s, many public, registered addresses were allocated to firms & organizations without any consistent control
- As a result, some organizations have more addresses that they actually might need
- Also, not all IP addresses can be used due to the fragmentation described previously

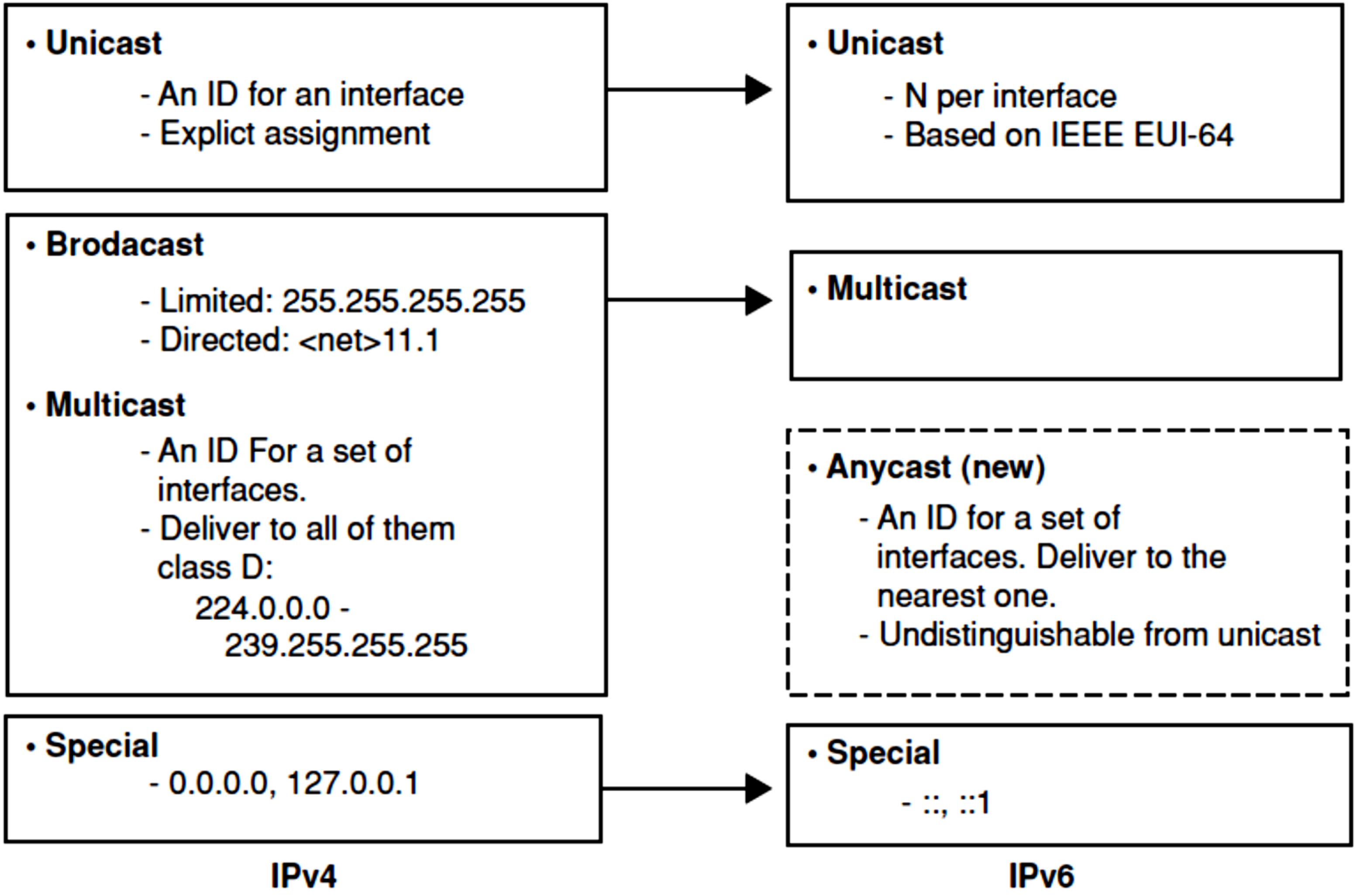
IPv4 Addressing and Issues

- One approach to issue would be renumbering and reallocation of the IPv4 addressing space
- But this is not as simple as it appears since it requires worldwide coordination efforts

IPv6 Address Space

- IPv6 addressing architecture is described in RFC 4291 February 2006
- One of the major modifications in addressing scheme in IPv6 is a change to the basic types of addresses and how they are utilized

Address Comparison between IPv4 & IPv6



- **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

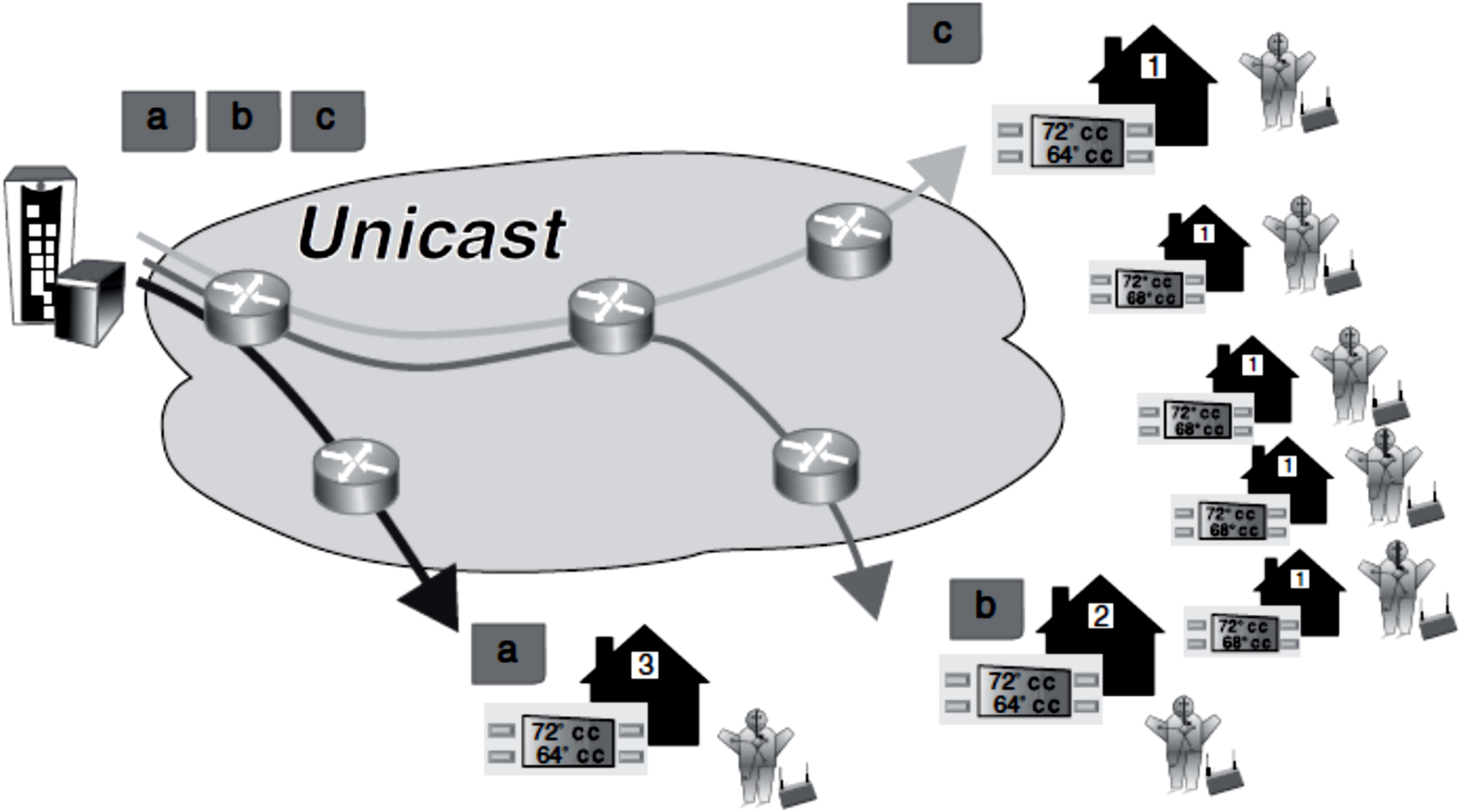
- **Special**
  - ::, ::1

IPv6

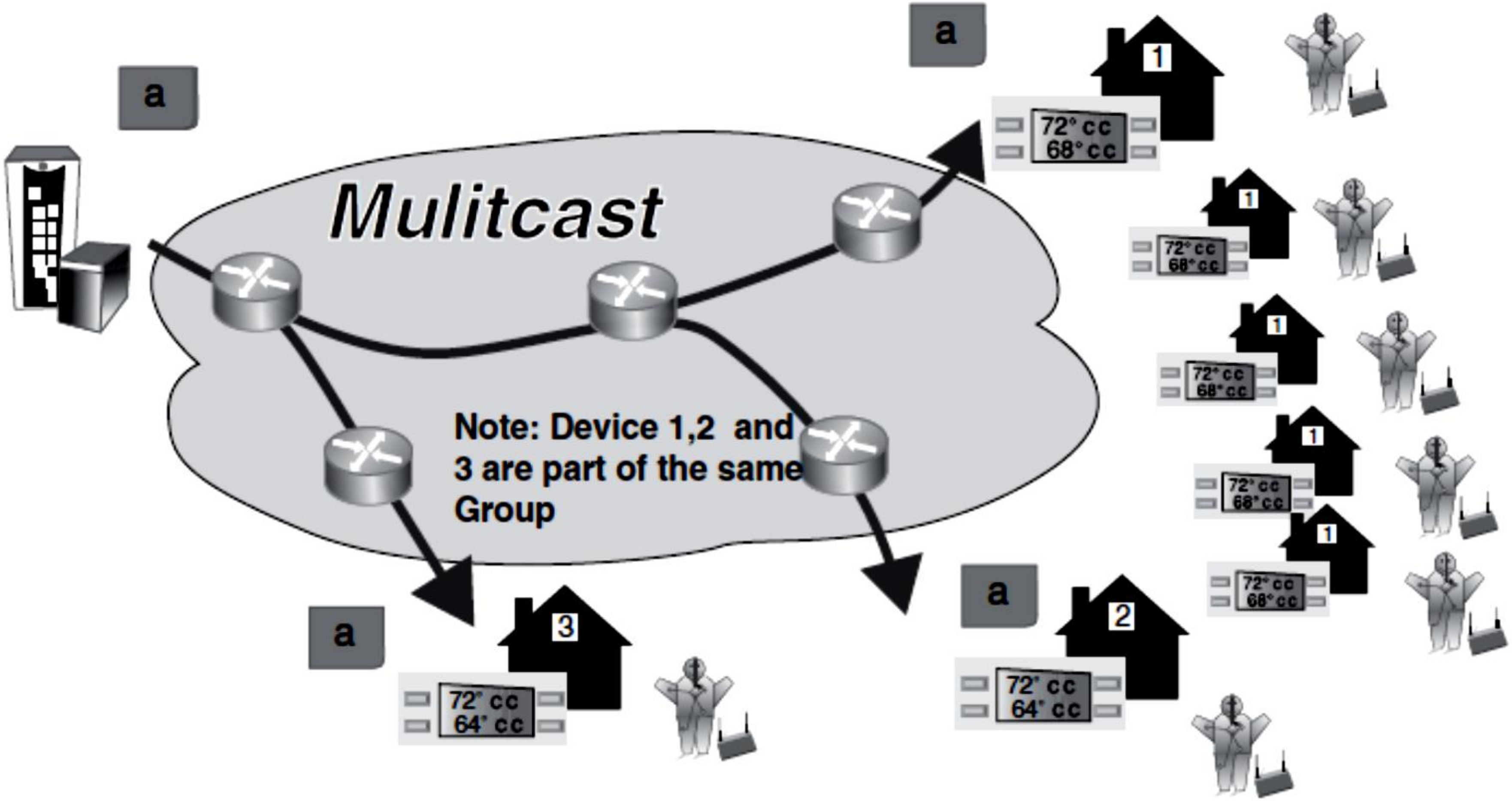
IPv6 Address Space

- Unicast : “send to this one specific address”
- Multicast : “send to every member of this specific group”
- Anycast : “send to any one member of this specific group.” Typically, the transmission occurs to closest member of group. Generally one interprets anycast to mean “send to the closest member of this specific group.”

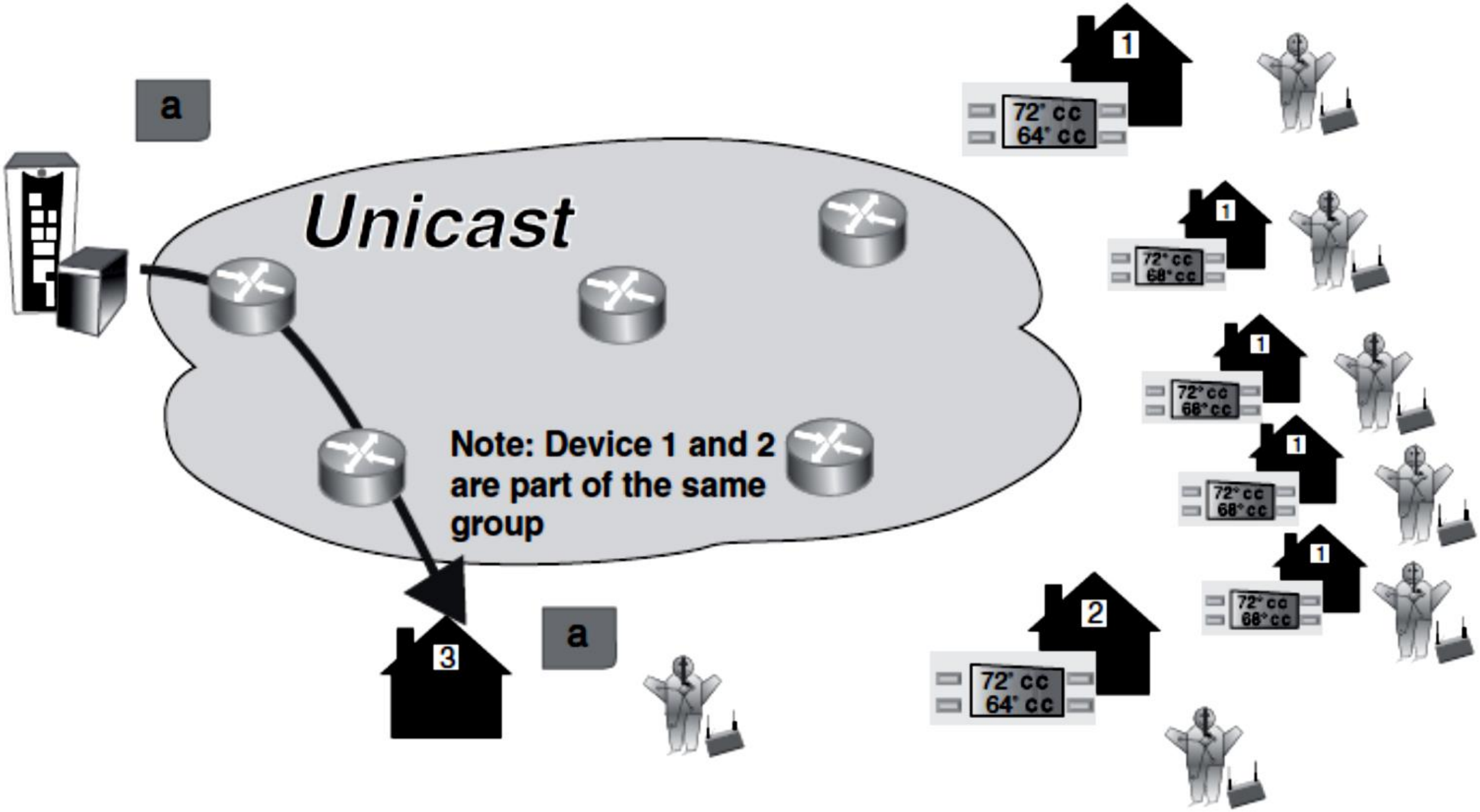
IPv6 Address Space



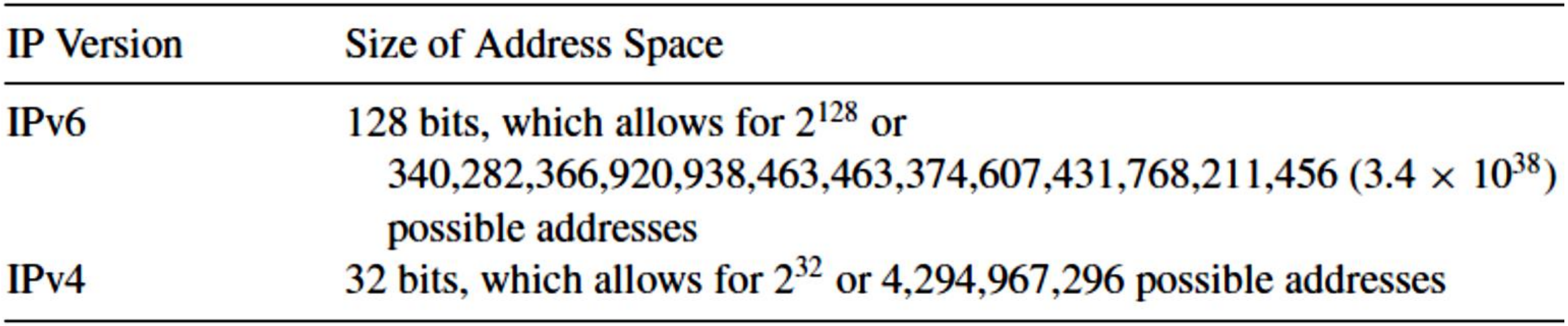
IPv6 Address Space



IPv6 Address Space

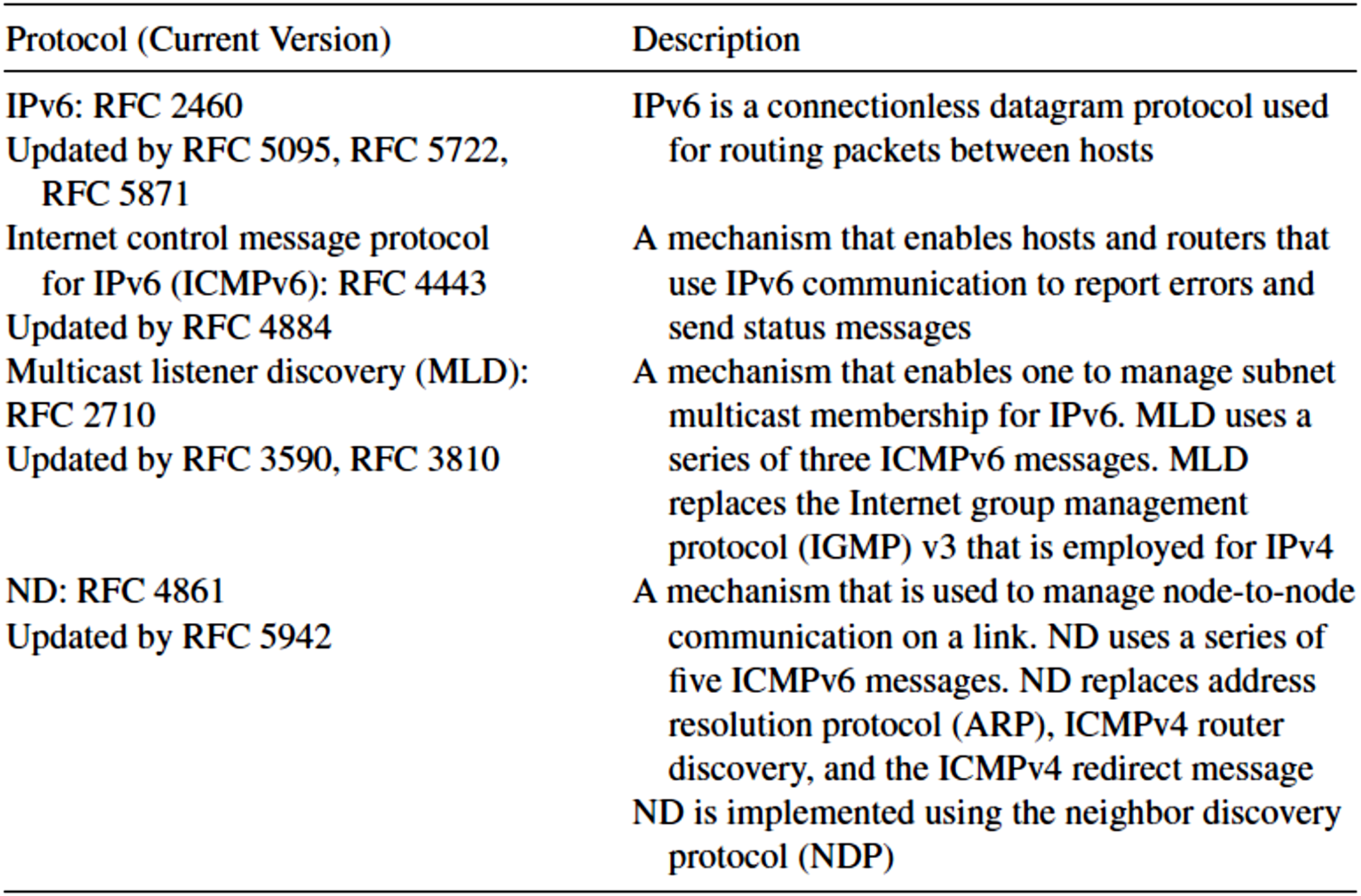


IPv6 Address Space



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

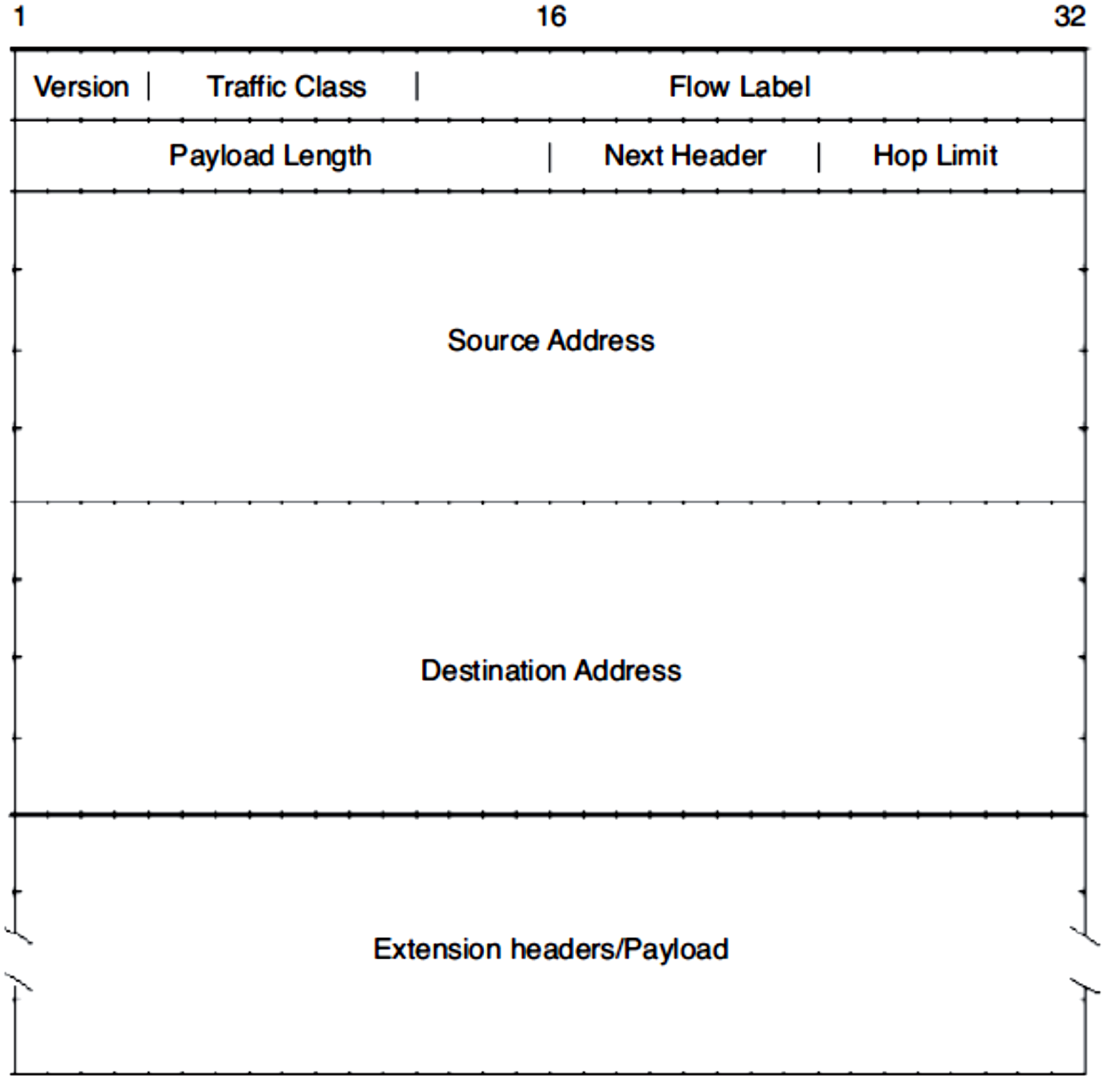


Protocol (Current Version)	Description
IPv6: RFC 2460 Updated by RFC 5095, RFC 5722, RFC 5871	IPv6 is a connectionless datagram protocol used for routing packets between hosts
Internet control message protocol for IPv6 (ICMPv6): RFC 4443 Updated by RFC 4884	A mechanism that enables hosts and routers that use IPv6 communication to report errors and send status messages
Multicast listener discovery (MLD): RFC 2710 Updated by RFC 3590, RFC 3810	A mechanism that enables one to manage subnet multicast membership for IPv6. MLD uses a series of three ICMPv6 messages. MLD replaces the Internet group management protocol (IGMP) v3 that is employed for IPv4
ND: RFC 4861 Updated by RFC 5942	A mechanism that is used to manage node-to-node communication on a link. ND uses a series of five ICMPv6 messages. ND replaces address resolution protocol (ARP), ICMPv4 router discovery, and the ICMPv4 redirect message ND is implemented using the neighbor discovery protocol (NDP)

IPv6 Protocol Overview

- IPv6 basic protocol capabilities include:
  - Addressing
  - Anycast
  - Flow Labels
  - ICMPv6
  - Neighbor discovery (ND)

IPv6 Packet



1 16 32

Version | Traffic Class | Flow Label

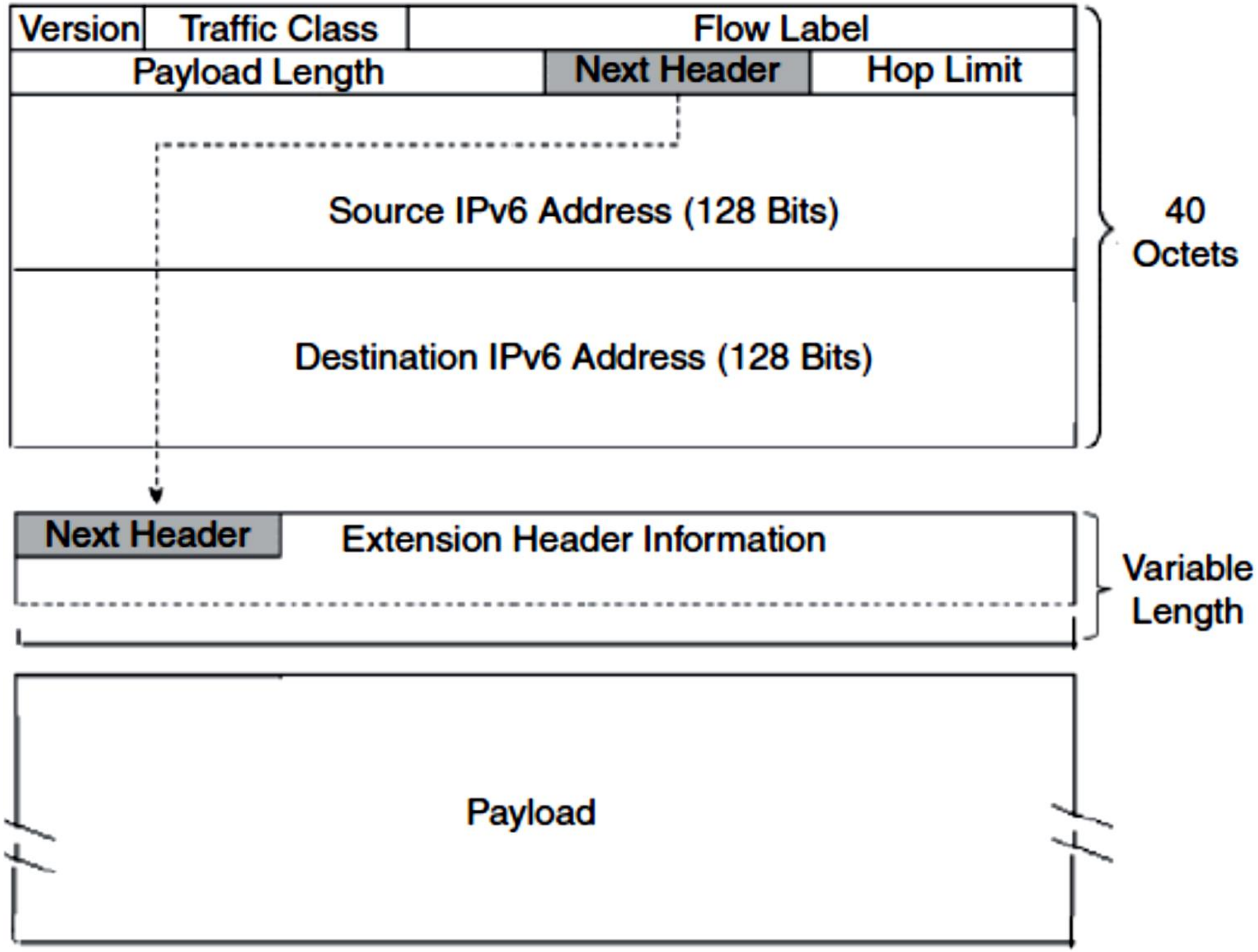
Payload Length | Next Header | Hop Limit

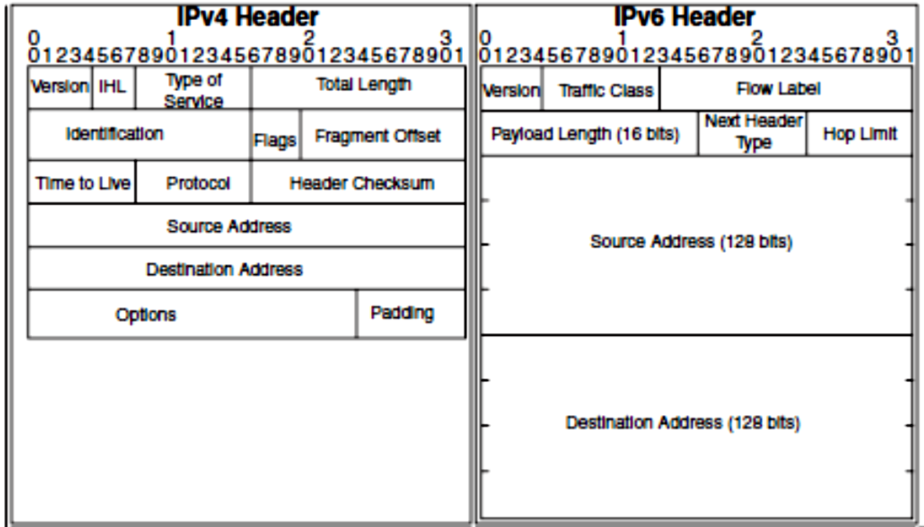
Source Address

Destination Address

Extension headers/Payload

IPv6 Extension Headers



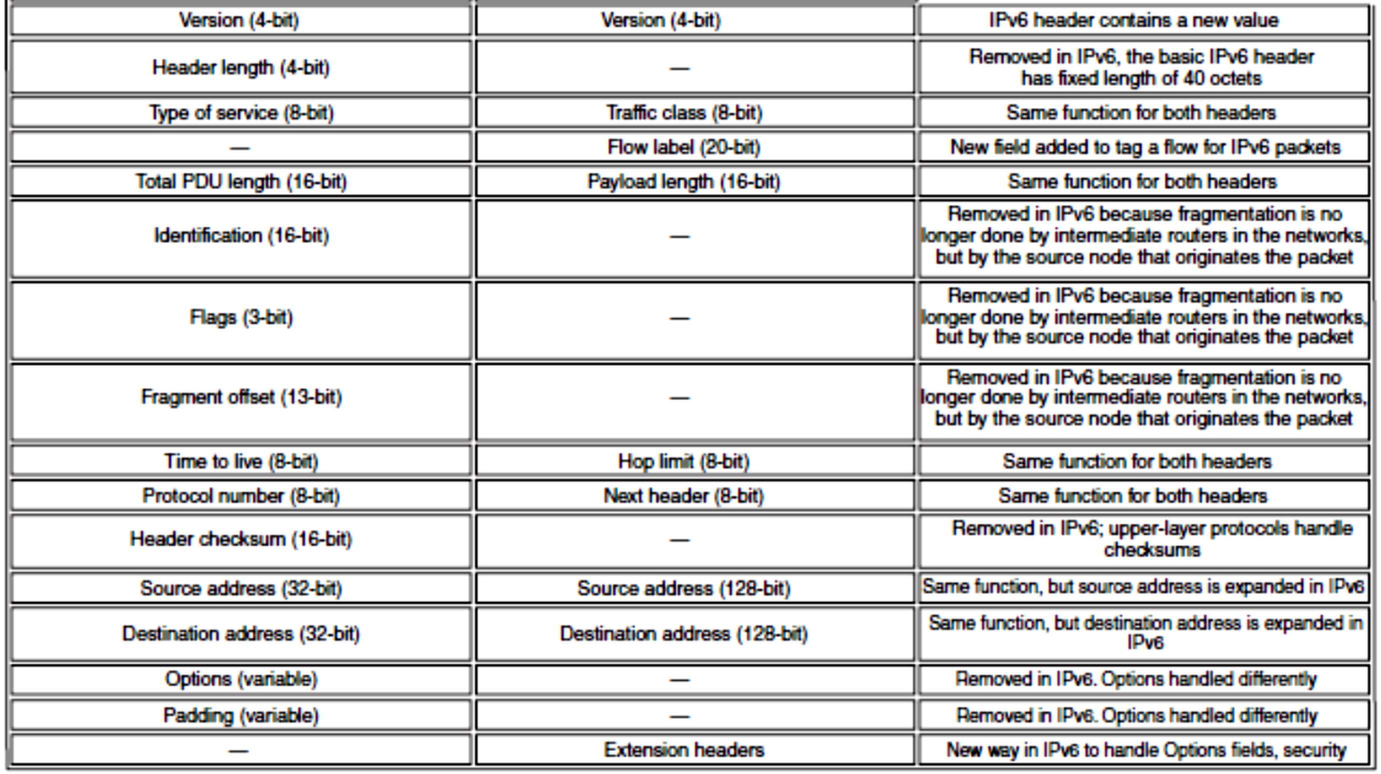


IPv4 Header

Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live	Protocol	Header Checksum	
Source Address			
Destination Address			
Options			Padding

IPv6 Header

Version	Traffic Class	Flow Label
Payload Length (16 bits)	Next Header Type	Hop Limit
Source Address (128 bits)		
Destination Address (128 bits)		



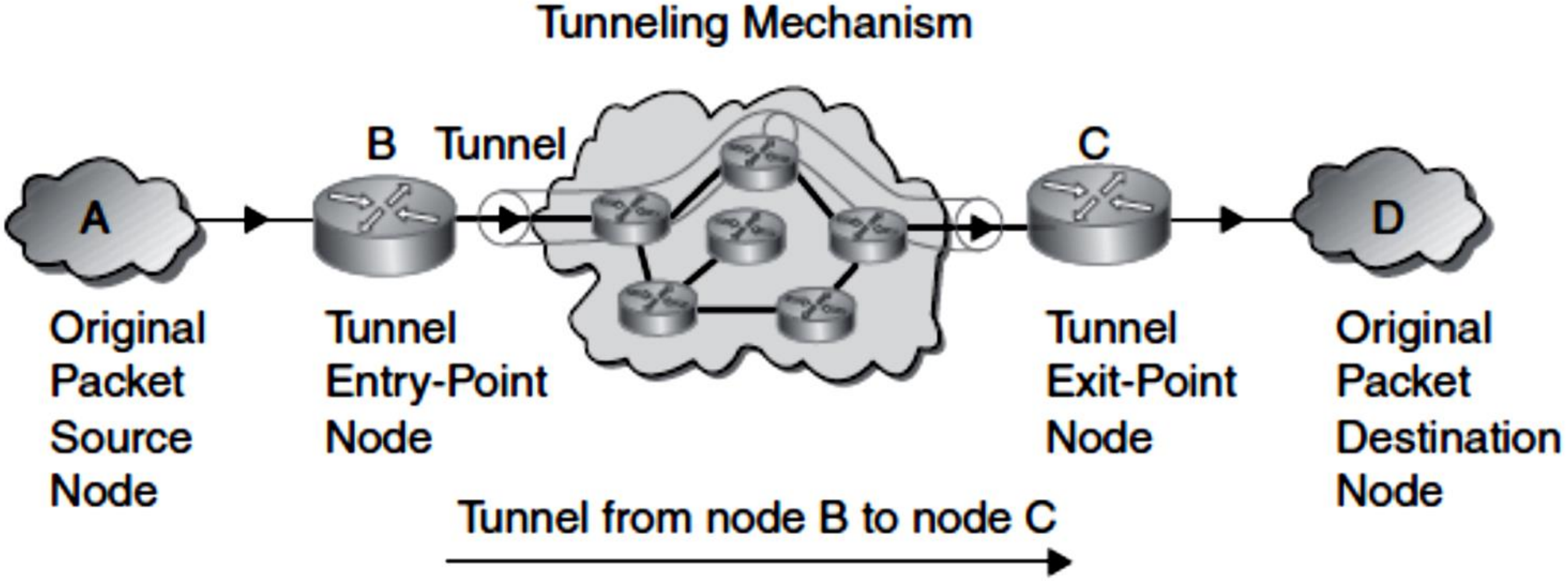
Version (4-bit)	Version (4-bit)	IPv6 header contains a new value
Header length (4-bit)	—	Removed in IPv6, the basic IPv6 header has fixed length of 40 octets
Type of service (8-bit)	Traffic class (8-bit)	Same function for both headers
—	Flow label (20-bit)	New field added to tag a flow for IPv6 packets
Total PDU length (16-bit)	Payload length (16-bit)	Same function for both headers
Identification (16-bit)	—	Removed in IPv6 because fragmentation is no longer done by intermediate routers in the networks, but by the source node that originates the packet
Flags (3-bit)	—	Removed in IPv6 because fragmentation is no longer done by intermediate routers in the networks, but by the source node that originates the packet
Fragment offset (13-bit)	—	Removed in IPv6 because fragmentation is no longer done by intermediate routers in the networks, but by the source node that originates the packet
Time to live (8-bit)	Hop limit (8-bit)	Same function for both headers
Protocol number (8-bit)	Next header (8-bit)	Same function for both headers
Header checksum (16-bit)	—	Removed in IPv6; upper-layer protocols handle checksums
Source address (32-bit)	Source address (128-bit)	Same function, but source address is expanded in IPv6
Destination address (32-bit)	Destination address (128-bit)	Same function, but destination address is expanded in IPv6
Options (variable)	—	Removed in IPv6. Options handled differently
Padding (variable)	—	Removed in IPv6. Options handled differently
—	Extension headers	New way in IPv6 to handle Options fields, security

IPv6 Tunneling

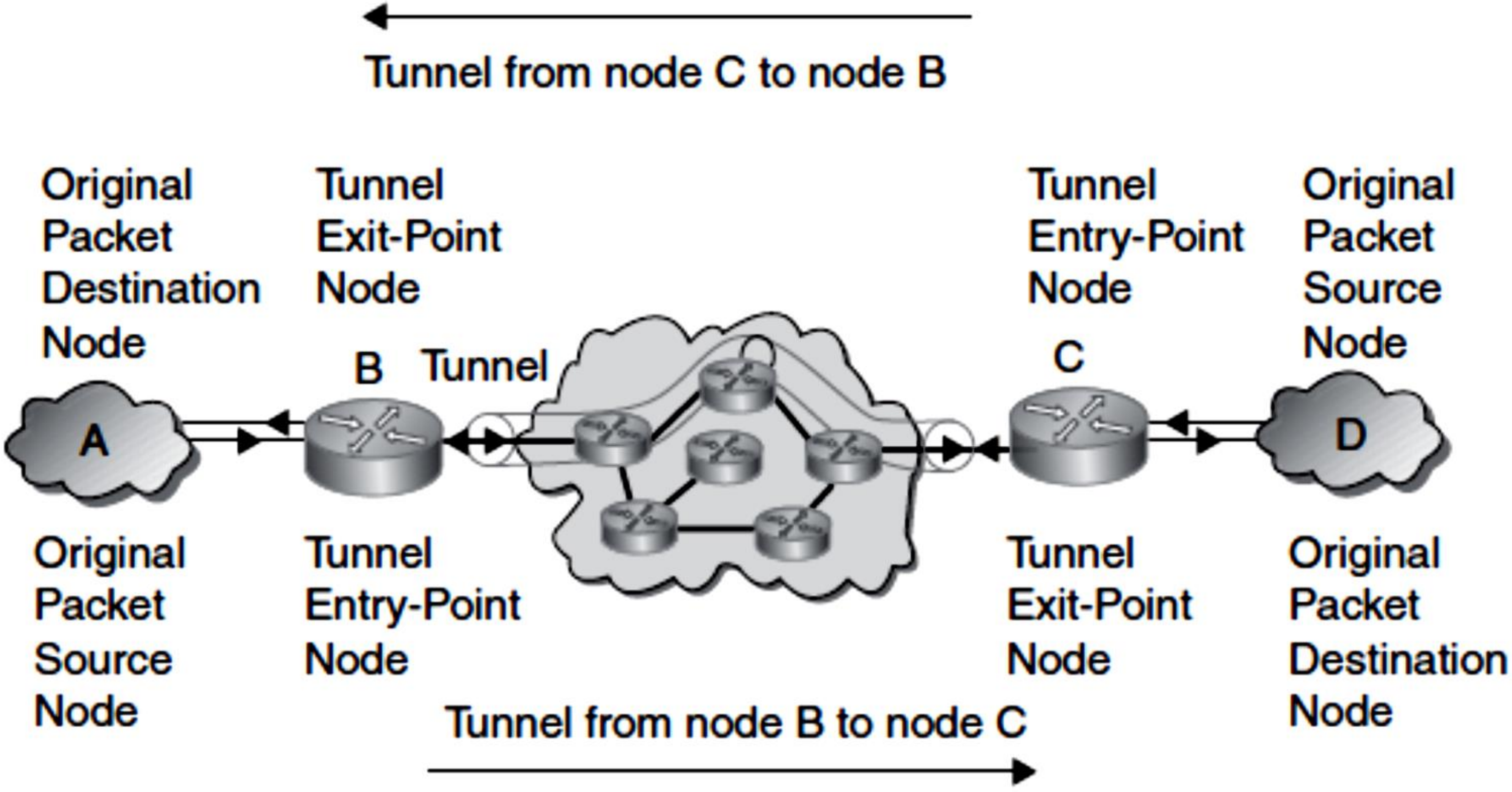
- Used in variety of settings, including in MIPv6
- MIPv6 tunnels payload packets between the mobile node (MN) and the home agent (HA) in both directions
- This tunneling uses IPv6 encapsulation
- IPv6 tunneling is defined in RFC 2473

Technique for establishing “virtual link” between two IPv6 nodes for transmitting data packets as payloads of IPv6 packets

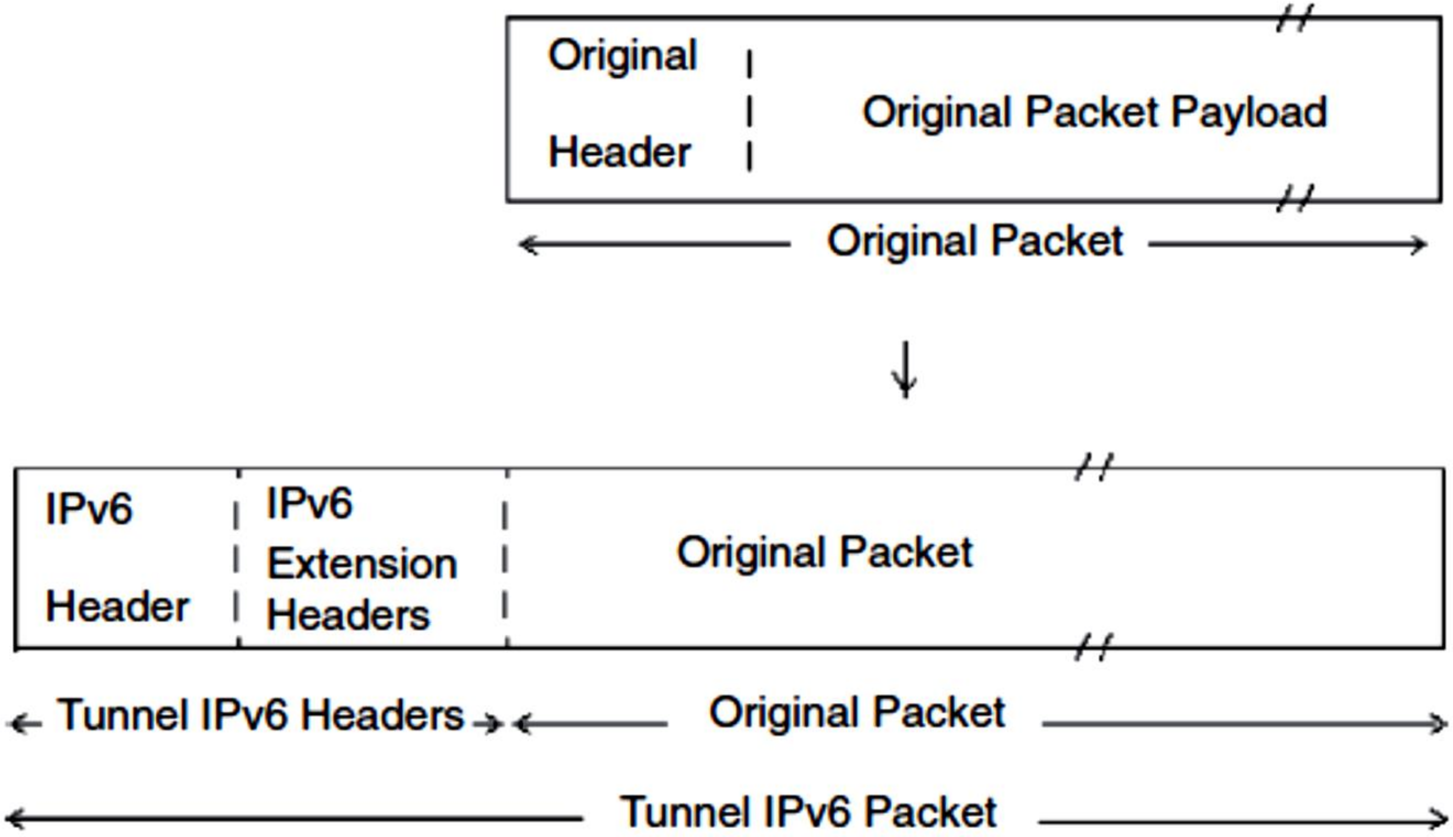
IPv6 Tunneling


Tunneling Mechanism
B
Tunnel
C
A
D
Original Packet Source Node
Tunnel Entry-Point Node
Tunnel Exit-Point Node
Original Packet Destination Node
Tunnel from node B to node C

IPv6 Tunneling


Tunnel from node C to node B
Original Packet Destination Node
Tunnel Exit-Point Node
Tunnel Entry-Point Node
Original Packet Source Node
B
Tunnel
C
A
D
Original Packet Source Node
Tunnel Entry-Point Node
Tunnel Exit-Point Node
Original Packet Destination Node
Tunnel from node B to node C

Encapsulating Packet



IPsec in IPv6

- IPsec provides network-level security where application data is encapsulated in IPv6 packet
- IPsec itself is a set of two protocols:
  - Encapsulating Security Payload (ESP)
  - Authentication Header (AH)
- ESP provides integrity & confidentiality and AH provides integrity

IPsec in IPv6

- Both AH and ESP header may be employed as:

Tunnel Mode

- The protocol is applied to the entire IP packet
- This method is needed to ensure security over the entire packet
- Here, a new IPv6 header and an AH or ESP header are wrapped around the original IP packet

Transport Mode

- The protocol is just applied to the transport layer (i.e., TCP, UDP, ICMP) in the form of an IPv6 header and AH or ESP header, followed by the transport protocol data (header, data)

Quality of Service in IPv6

- ETSI standards require that M2M system should be able to make use of QoS supported by underlying networks
- QoS is supported in IPv6
- The IPv6 header has two QoS-related fields

Quality of Service in IPv6

- 20-bit flow label, usable in IntServ-based environments. (In IntServ environments, performance guarantees to traffic and resource reservations are provided on per-flow basis)
- 8-bit traffic class indicator usable in DiffServ-based environments. (DiffServ environments are more common. The traffic class field may be used to set specific precedence or differentiated services code point (DSCP) values)

Quality of Service in IPv6

- There are no signaling protocol for resource allocation (admission control) and QoS mechanisms control
- The following priority levels are typical, but variances are possible:

Quality of Service in IPv6

- Level 0—No specify priority
- Level 1—Background traffic (news)
- Level 2—Unattended data transfer (email)
- Level 3—Reserved
- Level 4—Attended bulk transfer (FTP)
- Level 5—Reserved
- Level 6—Interactive traffic (Telnet, Windowing)
- Level 7—Control traffic (routing, network management)

Mobile IPV6 Technologies for the IoT: Protocol Details

- Recent Implementations on MIPv6 Technology
  - 6 Wind
  - Cisco—HA
  - Elmic systems now Treck Inc.
  - Ericsson
  - HP—HP-UX (HA, CN) and Tru64 (HA, CN)
  - Keio University (wide) —HA, MN, CN, and IPsec
  - Microsoft Window XP, Vista
  - NEC-MN, HA, CN, and IPsec
  - Nokia-MN, HA, CN
  - Samsung—MN, CN
  - Siemens
  - University of Helsinski (Linux) —MN, CN
  - 6NET MIPv6 implementation survey

Mobile IPV6 Technologies for the IoT: Protocol Details