UNIT III – THE NETWORK LAYER

Functions of the Network Layer: Logical addressing, routing, and forwarding. IP addressing: IPv4 and IPv6.Routing algorithms: Distance vector, link state, and path vector. Routers and their role in packet forwarding and routing., Applications: BGP in global internet routing, OSPF in ISPs, IPv6 in IoT, routers in enterprise edge networks, dynamic routing in disaster response networks

1. FUNCTIONS OF THE NETWORK LAYER: LOGICAL ADDRESSING, ROUTING, AND FORWARDING

- Functions of the Network Layer:
    - *Logical addressing*
    - *Routing*
    - *Forwarding*

Logical Addressing

- In computer networks, every device connected to the internet needs a *unique identification.*
- Logical Addressing is the method used *to give every device an IP address* so that data can be sent and received correctly

What is Logical Addressing?

- Logical Addressing is *the process of assigning a logical number (IP)* to every device on a network.
- This IP address is not linked to the hardware of the device permanently, but it is assigned to the device whenever it connects to a network.
- This address can change if the device connects to a different network. Logical Addressing happens at the Network Layer of the OSI Model.

Why do we need Logical Addressing?

- We need Logical Addressing because billions of devices exist worldwide, and without a proper logical structure, it would be impossible for devices to communicate globally.
- Logical addresses help routers identify the source device and the destination device on the internet.
- When you open a website, your device needs to know the server's address and the server needs to know your device's address.
- Logical addressing makes this communication possible.

What is the difference between Logical Address and Physical Address?

- A logical address is the IP address that is used for communication over the internet. It helps in routing data between different networks. It can change depending on the network you connect to.

- A physical address (MAC address) is permanently assigned to the device's network card and does not change. It is used only inside the local network. So in simple words, logical address works globally across the internet, and physical address works locally inside your own network.

Routing and Forwarding

- **Routing**
  - Is responsible for routing the packet from its source to the destination.
  - A ***physical network*** is a combination of networks (LANs and WANs) and ***routers*** that connect them.
  - Is responsible for finding the best one among these possible routes.
  - Needs to have some specific strategies for defining the best route.
  - Done by running some ***routing protocols*** to help the routers coordinate their knowledge about the neighborhood and to come up with consistent tables to be used when a packet
- **Forwarding**
  - Defined as the ***action applied by each router*** when a packet arrives at one of its interfaces.
  - The ***decision-making table*** a router normally uses for applying this action is called the ***forwarding table or routing table.***
  - When a router receives a packet from one of its attached networks, it needs to forward the packet to another attached network or to some attached networks.
  - Router uses a piece of information in the packet header, destination address or a label, to find the corresponding output interface number in the forwarding table.

Other services

a) Error Control

- In the Internet ignored this issue for the data being carried by the network layer.
- Packet in the network layer may be fragmented at each router, which makes error checking at this layer inefficient.
- The designers of the network layer, added a checksum field to the datagram to control any corruption in the header, but not in the whole datagram.
- Checksum may prevent any changes or corruptions in the header of the datagram.
- Internet uses an auxiliary protocol, ICMP, that provides some kind of error control if the datagram is discarded or has some unknown information in the header.

b) Flow Control

- If the upper layer at the source computer produces data faster than that at the destination computer can consume it, the receiver will be overwhelmed with data.
- To control the flow of data, the receiver needs to send some feedback to the sender to inform the latter that it is overwhelmed with data.
- Reasons for lack of flow control in the network layer:
- First, since there is no error control in this layer, the receiver may rarely be overwhelmed.
- Second, the upper layers that use the service of the network layer can implement buffers to receive data from the network layer as they are ready and do not have to consume the data as fast as it is received.
- Third, flow control is provided for most of the upper-layer protocols that use the services of the network layer.

c) Congestion Control

- Is a situation in which too many datagrams are present in an area of the Internet.
- May occur if the number of datagrams sent by source computers is beyond the capacity of the network or routers. In this situation, some routers may drop some of the datagrams.
- As more datagrams are dropped, the situation may become worse because, due to the error control mechanism at the upper layers, the sender may send duplicates of the lost packets.
- If the congestion continues, sometimes a situation may reach a point where the system collapses and no datagrams are delivered.

d) Quality of Service

- Has allowed new applications such as multimedia communication, the quality of service (QoS) of the communication has become more and more important.
- Internet has thrived by providing better quality of service.

e) Security

- When the Internet was originally designed because it was used by a small number of users.
- To provide security for a connectionless network layer, we need to have another virtual level that changes the connectionless service to a connection-oriented service.
- This virtual layer, called IPSec service to support these applications.

2. IP ADDRESSING: IPV4 AND IPV6

IPV4:

- The ***identifier*** used in the IP layer of the TCP/IP protocol suite to ***identify the connection*** of each device to the Internet is called the Internet address or IP address.
    - Internet Protocol version 4 (IPv4) is the fourth version in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed.
    - IPv4 is described in IETF publication in September 1981.

- The IP address is the ***address of the connection***, not the host or the router. An IPv4 address is a ***32-bit address*** that uniquely and universally defines the connection.
- If the device is moved to another network, the IP address may be changed.
- IPv4 addresses are unique in the sense that each address defines one, and only one, connection to the Internet.
- If a device has two connections to the Internet, via two networks, it has two IPv4 addresses.
- IPv4 addresses are universal in the sense that the addressing system must be accepted by any host that wants to be connected to the Internet.

IPV4 ADDRESS SPACE

- IPv4 defines addresses has an ***address space***.
- An address space is the total number of addresses used by the protocol.
- If a protocol uses *b bits to define an address, the address space is 2^b* because each bit can have two different values (0 or 1).
- IPv4 uses 32-bit addresses, which means that the address space is 2^32 Or 4,294,967,296 (more than four billion).
- 4 billion devices could be connected to the Internet.

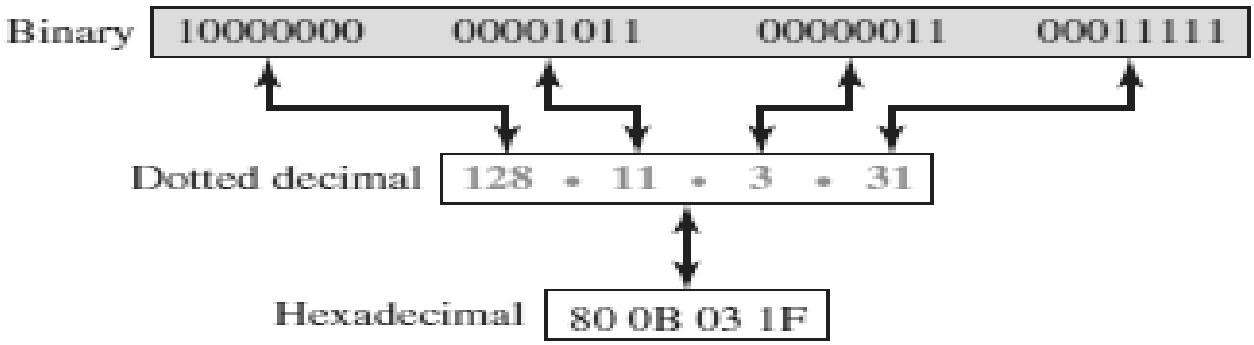
IPV4 ADDRESS NOTATION

- There are three common notations to show an IPv4 address:

(i) binary notation (base 2),

(ii) dotted-decimal notation (base 256), and

(iii) hexadecimal notation (base 16).

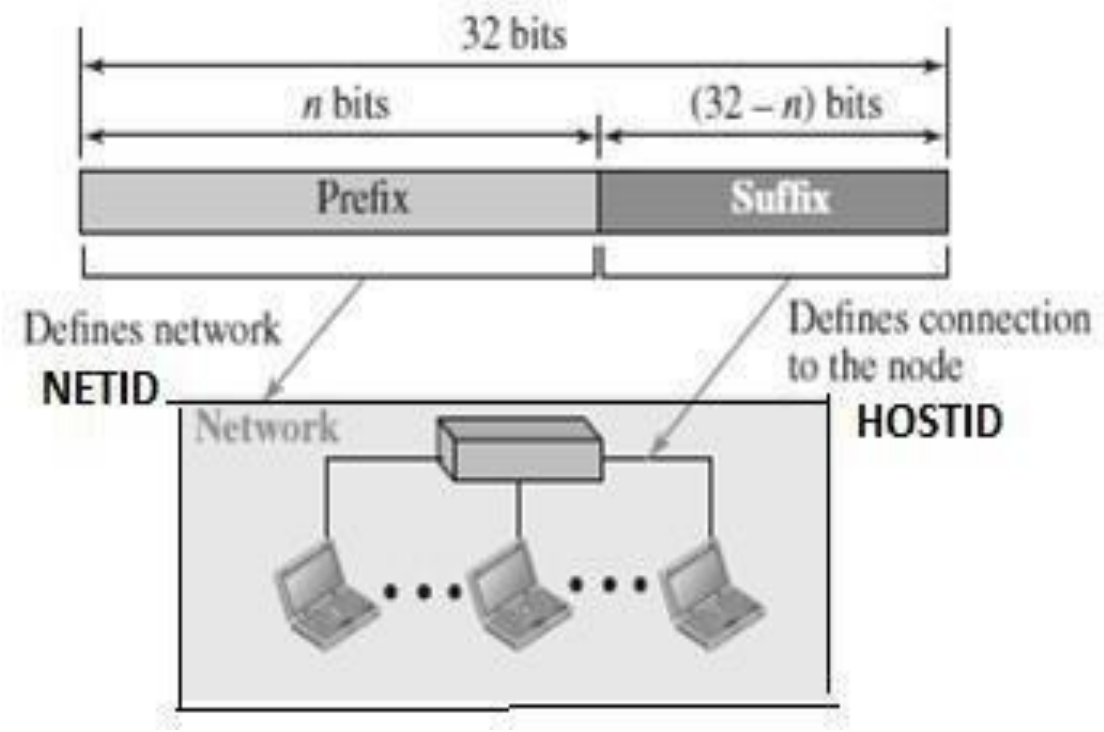


- In *binary notation, an IPv4 address is displayed as 32 bits. To make the address more* readable, one or more spaces are usually inserted between bytes (8 bits).

- In *dotted-decimal notation, IPv4 addresses are usually written in decimal form with a* decimal point (dot) separating the bytes. Each number in the dotted-decimal notation is between 0 and 255.
- In hexadecimal notation, each hexadecimal digit is equivalent to four bits. This means that a 32-bit address has 8 hexadecimal digits. This notation is often used in network programming.

HIERARCHY IN IPV4 ADDRESSING

- In any communication network that involves delivery, the addressing system is hierarchical.
- A 32-bit IPv4 address is also hierarchical, but divided only into two parts.
- The **first part** of the address, called the ***prefix***, *defines the network (Net ID); the* **second part** of the address, called the ***suffix***, *defines the node (Host ID).*
    - The prefix length is *n bits and the suffix length is (32- n) bits.*



- A prefix can be ***fixed length or variable length***.

· The network identifier in the IPv4 was first designed as a fixed-length prefix.

· This scheme is referred to as ***classful addressing*** (fixed length prefix).

· The new scheme, which is referred to as ***classless addressing***, uses a variable-length network prefix

CATEGORIES OF IPV4 ADDRESSING

There are two broad categories of IPv4 Addressing techniques.

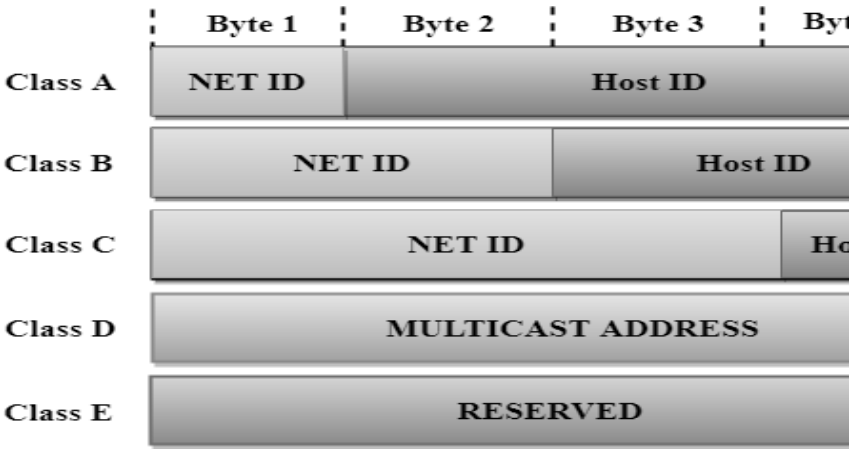
· They are

Ø Classful Addressing

Ø Classless Addressing

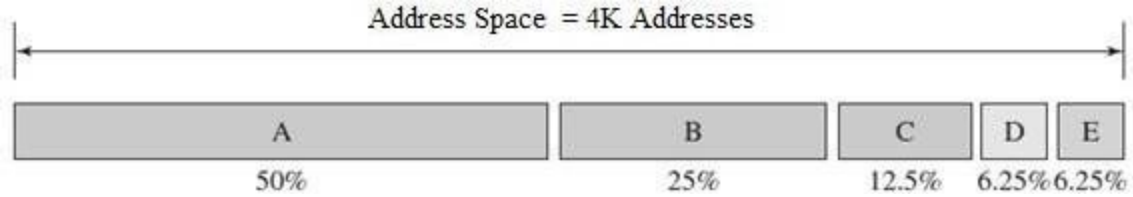
CLASSFUL ADDRESSING

- An IPv4 address is 32-bit long (4 bytes).
  - · An IPv4 address is divided into sub-classes:



Class	Prefixes	First byte
A	*n* = 8 bits	0 to 127
B	*n* = 16 bits	128 to 191
C	*n* = 24 bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

Classful Network Architecture



Class	Higher bits	NET ID bits	HOST ID bits	No. of Networks	No.of hosts per network	Range
A	0	8	24	2^7	2^{24}	0.0.0.0 **to** 127.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 **to** 191.255.255.255
C	110	24	8	2^{21}	2^8	192.0.0.0 **to** 223.255.255.255
D	1110	Not Defined	Not Defined	Not Defined	Not Defined	224.0.0.0 **to** 239.255.255.255
E	1111	Not Defined	Not Defined	Not Defined	Not Defined	240.0.0.0 **to** 255.255.255.255

Class A

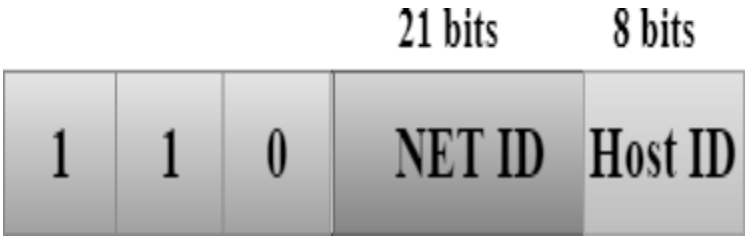
- In Class A, an IP address is assigned to those networks that contain a ***large number of hosts.***
  - The network ID is 8 bits long.
  - The host ID is 24 bits long.
- In Class A, the ***first bit*** in higher order bits of the first octet is ***always set to 0*** and the remaining 7 bits determine the network ID.
  - The 24 bits determine the host ID in any network.
  - The total number of networks in Class A = 2 ^7 = 128 network address
  - The total number of hosts in Class A = 2 ^24 - 2 = 16,777,214 host address

Class B

- In Class B, an IP address is assigned to those networks that range from ***small sized to large-sized networks***.
  - The Network ID is 16 bits long.
  - The Host ID is 16 bits long.
- In Class B, the higher order bits of the first octet is ***always set to 0 1***, and remaining14 bits determine the network ID.
  - The other 16 bits determine the Host ID.
  - The total number of networks in Class B = 2 ^14 = 16384 network address
  - The total number of hosts in Class B = 2 ^16 - 2 = 65534 host address

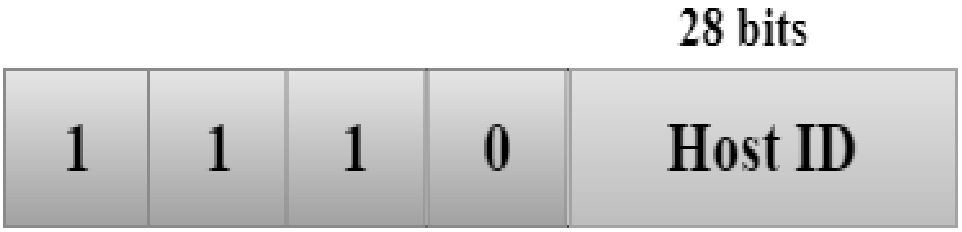
Class C

- In Class C, an IP address is assigned to only small-sized networks.
  - The Network ID is 24 bits long.
  - The host ID is 8 bits long.
  - In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID.
  - The 8 bits of the host ID determine the host in a network.
  - The total number of networks = 2^21 = 2097152 network address
  - The total number of hosts = 2 ^8 - 2 = 254 host address



Class D

- In Class D, an IP address is reserved for multicast addresses.
    - It does not possess subnetting.
    - The higher order bits of the set to 1110, and the remaining bits determines the host ID in any network.



Class E

- In Class E, an IP address is used for the future use or for the research and development purposes.
    - It does not possess any subnetting.
    - The higher order bits of the first octet are always set to 1111, and the remaining bits determines the host ID in any network.

<u>Address Depletion in Classful Addressing</u>

- The reason that classful addressing has become obsolete is address depletion.
    - Since the ***<u>addresses were not distributed properly</u>***, the Internet was faced with the problem of the addresses being rapidly used up.
    - This results in no more addresses available for organizations and individuals that needed to be connected to the Internet.
    - To understand the problem, let us think about class A.
    - This class can be assigned to only 128 organizations in the world, but each organization needs to have a single network with 16,777,216 nodes.
    - Since there may be only a few organizations that are this large, most of the addresses in this class were wasted (unused).

- Class B addresses were designed for midsize organizations, but many of the addresses in this class also remained unused.
- Class C addresses have a completely different flaw in design. The number of addresses that can be used in each network (256) was so small that most companies were not comfortable using a block in this address class.
- Class E addresses were almost never used, wasting the whole class.

Subnetting and Supernetting

· To alleviate address depletion, two strategies were proposed and implemented:

(i) Subnetting and

(ii) Supernetting

Subnetting

- A class A or class B block is divided into several subnets.
- Each subnet has a larger prefix length than the original network. For example, if a network in class A is divided into four subnets, each subnet has a prefix of nsub = 10.
- At the same time, if all of the addresses in a network are not used, subnetting allows the addresses to be divided among several organizations.
- This idea did not work because most large organizations were not happy about dividing the block and giving some of the unused addresses to smaller organizations.
- While subnetting was devised to divide a large block into smaller ones.

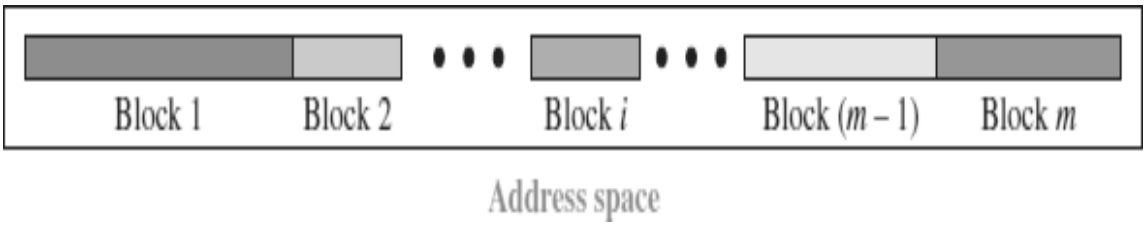
Supernetting

- Was devised to combine several class C blocks into a larger block to be attractive to organizations that need more than the 256 addresses available in a class C block.
- This idea did not work either because it makes the routing of
- packets more difficult.
- Advantage of Classful Addressing
- Given an address, can easily find the class of the address, since the prefix length for each class is fixed, can find the prefix length immediately.

CLASSLESS ADDRESSING

- In 1996, the Internet authorities announced a new architecture called **classless addressing.**
  - In classless addressing, variable-length blocks are used that belong to no classes.
  - We can have a block of 1 address, 2 addresses, 4 addresses, 128 addresses, and so on.
  - In classless addressing, the whole address space is divided into variable length blocks.
  - The prefix in an address defines the block (network); the suffix defines the node (device).

- Theoretically, we can have a block of 2^0, 2^1, 2^2, ……,2^32 addresses.
- The number of addresses in a block needs to be a power of 2. An organization can be granted one block of addresses.

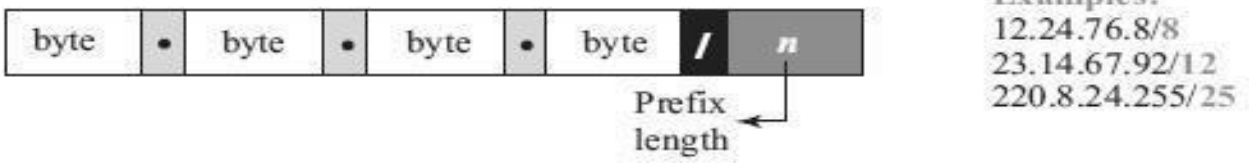


.

- The prefix length in classless addressing is variable.
  - We can have a prefix length that ranges from 0 to 32.
  - The size of the network is inversely proportional to the length of the prefix.
  - A small prefix means a larger network; a large prefix means a smaller network.
  - The idea of classless addressing can be easily applied to classful addressing.
  - An address in class A can be thought of as a classless address in which the prefix length is 8.
  - An address in class B can be thought of as a classless address in which the prefix is 16, and so on. In other words, classful addressing is a special case of classless addressing.

<u>Notation used in Classless Addressing</u>

- The notation used in classless addressing is informally referred to as *slash notation and formally as* ***classless inter domain routing or CIDR.***



For example, 192.168.100.14 **/24 represents the IP address 192.168.100.14** and, its subnet mask 255.255.255.0, which has 24 leading 1-bits.

<u>Address Aggregation</u>

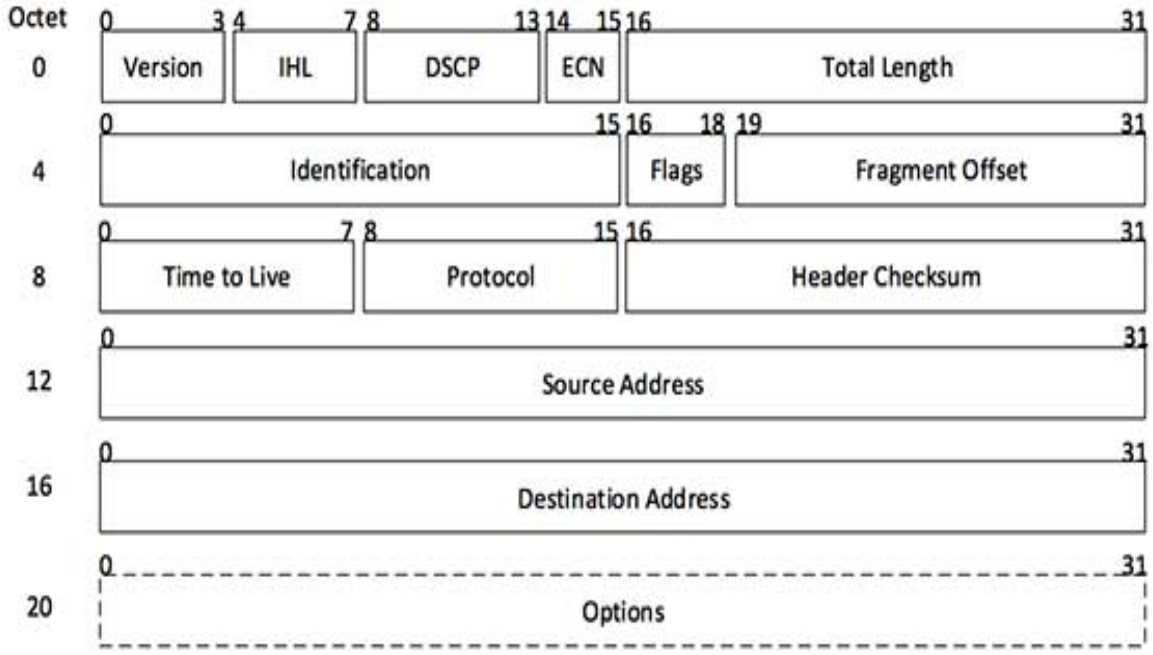
- One of the advantages of the CIDR strategy is **address aggregation** (Sometimes called *address summarization or route summarization).*
  - When blocks of addresses are combined to create a larger block, routing can be done based on the prefix of the larger block.
- ICANN assigns a large block of addresses to an ISP.

- Each ISP in turn divides its assigned block into smaller subblocks and grants the subblocks to its customers.

Special Addresses in IPv4

- There are five special addresses that are used for special purposes: *this-*
  - *host address,*
  - *limited-broadcast address,*
  - *loopback address,*
  - *private addresses,*
  - *multicast addresses*

IPv4 Datagram Header



[Image: IP Header]

Version − Version no. of Internet Protocol used (e.g. IPv4).

IHL − Internet Header Length; Length of entire IP header.

DSCP − Differentiated Services Code Point; this is Type of Service.

ECN − Explicit Congestion Notification; It carries information about the congestion seen in the route.

Total Length − Length of entire IP Packet (including IP header and IP Payload).

Identification − If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.

Flags − As required by the network resources, if IP Packet is too large to handle, these flags tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to 0.

Fragment Offset − This offset tells the exact position of the fragment in the original IP Packet.

Time to Live − To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.

Protocol − Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.

Header Checksum − This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.

Source Address − 32-bit address of the Sender (or source) of the packet.

Destination Address − 32-bit address of the Receiver (or destination) of the packet.

Options − This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

IPV6

i) Representation

- Uses 128 bit address and uses two notations: binary and colon hexadecimal.
- Binary notation is used when the addresses are stored in a computer.
- In colon hexadecimal notation divides the address into eight sections, each made
- of four hexadecimal digits separated by colons.

FDEC:0:0:0:0:BBFF:0:FFFF ⟶ FDEC::BBFF:0:FFFF

ii) Abbreviation

- Although an IPv6 address, even in hexadecimal format, is very long, many of the
- digits are zeros.
- 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.
- Zero compression, can be applied to colon hex notation, if there are consecutive sections consisting of zeros only. We can remove all the zeros and replace them with a double semicolon.

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

iii) Mixed Notation

- Sometimes uses colon hex and dotted decimal notation.
- Is appropriate during the transition period in which an IPv4 address is embedded in an IPv6 address (as the rightmost 32 bits).
- We can use the colon hex notation for the leftmost six sections and four-byte dotted-decimal notation instead of the rightmost two sections.
- The address (::130.24.24.18) is a legitimate address in IPv6, in which the zero compression shows that all 96 leftmost bits of the address are zeros.

iv) CIDR Notation

- IPv6 uses hierarchical addressing.
- IPv6 allows slash or CIDR notation.

FDEC::BBFF:0:FFFF/60

v) Address Space

- Contains 2128 addresses.
- Is 296 times the IPv4 address.
- Definitely no address depletion—as shown, the size of the space is

340, 282, 366, 920, 938, 463, 374, 607, 431, 768, 211, 456.

- The number of people on the earth is soon to be 234 (more than 16

billion).

- Each person can have 288 addresses to use.
- Three Address Types
- In IPv6, a destination address can belong to one of three categories:
  1. unicast,
  2. anycast, and
  3. multicast.

Unicast Address

- A unicast address defines a single interface.
- The packet sent to a unicast addresswill be routed to the intended recipient..

Anycast Address

- Defines a group of computers that all share a single address.
- A packet with an anycastaddressis delivered to only one member of the group, the most reachable one.
- The request is sent to the one that is most reachable.
- The addresses are assigned from the unicast block.

Multicast Address

- Defines a group of computers.
- 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.
- IPv6 has designated a block for multicasting from which the
- same address is assigned to the members of the group.
- IPv6 considers broadcasting as a special case of multicasting.

vi) Address Space Allocation

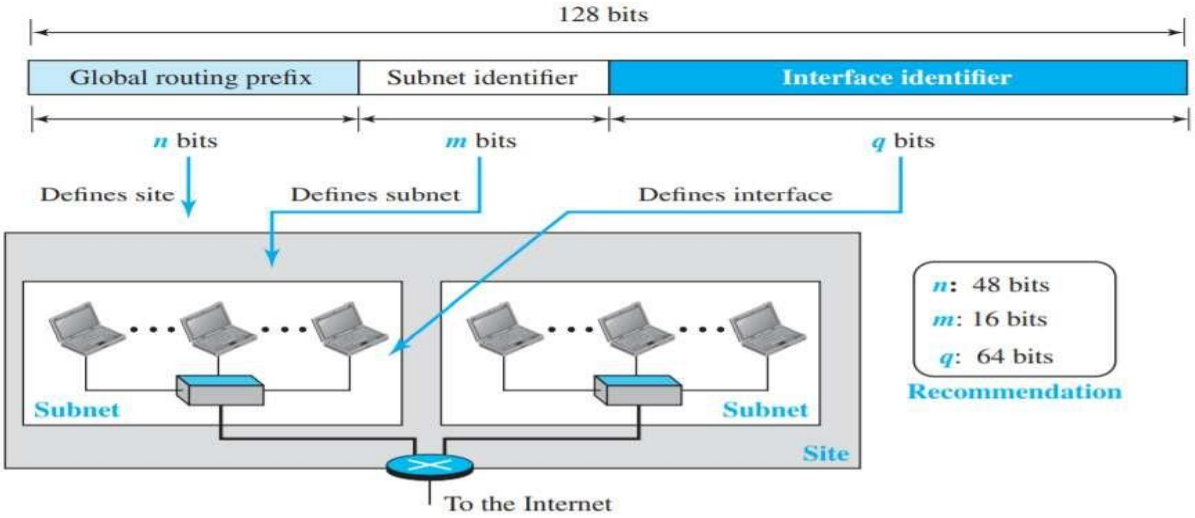
- Like the address space of IPv4, the address space of IPv6 is divided into several blocks of varying size and each block is allocated for a special purpose.
- Most of the blocks are still unassigned and have been set aside for future use.

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

a) Global Unicast Addresses

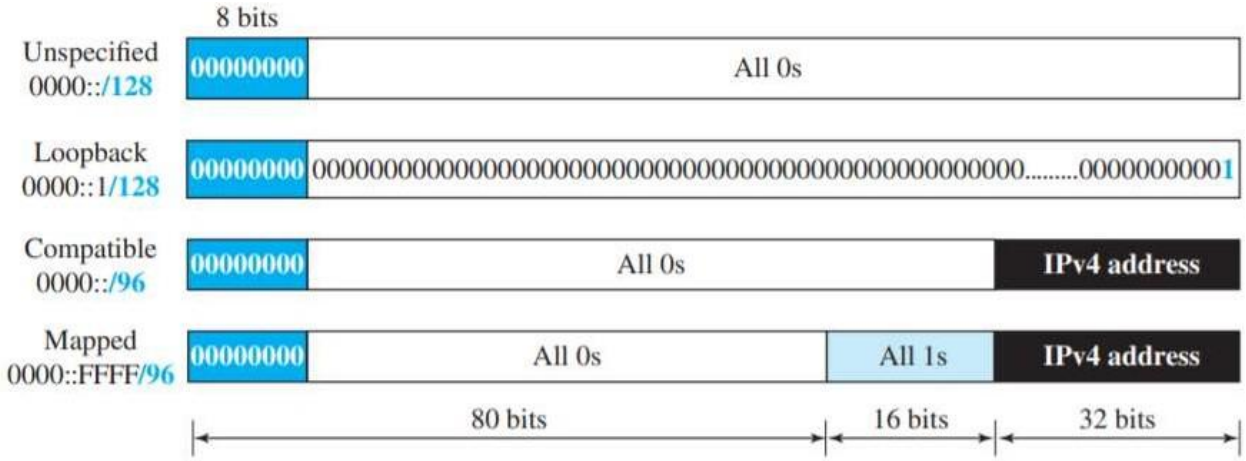
- The block in the address space is used for unicast (one-to-one) communication
- between two hosts in the Internet is called the Global Unicast Address Block.
- CIDR for the block is 2000::/3, which means that the three leftmost bits are the

- same for all addresses in this block (001).
- An address in this block is divided into three parts: global routing prefix (n bits),
- subnet identifier (m bits), and interface identifier (q bits).



b) Special Addresses

Addresses that use the prefix (0000::/8) are reserved, but part of this block is used to define some special addresses.



c) Auto configuration

- One of the interesting features of IPv6 addressing is the auto configuration of hosts.
- DHCP protocol can still be used to allocate an IPv6 address to a
- host, but a host can also configure itself.

d) Renumbering

- To allow sites to change the service provider, renumbering of the address
- prefix (n) was built into IPv6 addressing.
- If the site changes the provider, the address prefix needs to be changed.
- A router to which the site is connected can advertise a new prefix and let
- the site use the old prefix for a short time before disabling it.
- Needs support of the DNS, which needs to propagate the new addressing
- associated with a domain name.
- A new protocol for DNS, called Next Generation DNS, is under study to
- provide support for this mechanism.

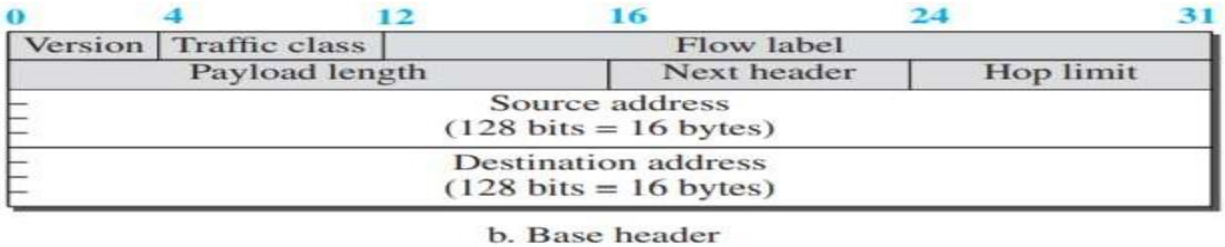
INTRODUCTION

- Support for resource allocation.
- Two new fields, traffic class and flow label, have been added to enable the source to request special handling of the packet.
- Can be used to support traffic such as real-time audio and video.
- Support for more security.
- The encryption and authentication optionsin 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.

a. IPv6 packet



b. Base header

- 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.
- 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. Defines two fields related to the length: header length fixed (40 bytes) and total length.
- 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-The source addressfield 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-Payload field in IPv6 has a different format and meaning.

ii) Concept of Flow and Priority in IPv6

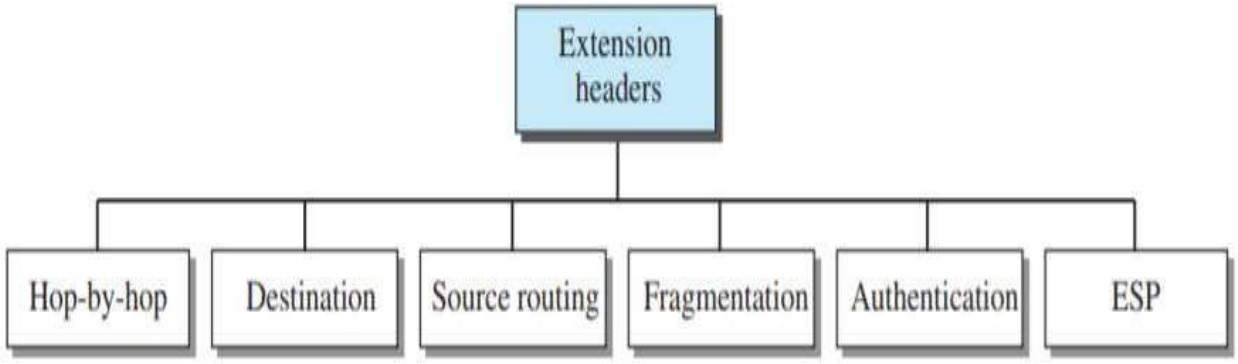
- The flow label has been directly added to the format of the IPv6 datagram to allow us to use IPv6 as a connection-oriented protocol.
- To a router, a flow is a sequence of packets that share the same characteristics, such as traveling the same path, using the same resources, having the same kind of security, and so on.
- **A router has a flow label table, that has an entry for each active flow label; each entry defines the services required by the corresponding flow label.**
- When the router receives a packet, it consults its flow label table to find the corresponding entry for the flow label value defined in the packet. It then provides the packet with the services mentioned in the entry.
- In its simplest form, a flow label can be used to speed up the processing of a packet by a router.

iii) Fragmentation and Reassembly

- IPv6 datagrams can be fragmented only by the source, not by the routers; the reassembly takes place at the destination.
- The fragmentation of packets at routers is not allowed to speed up the processing of packets in the router.
- In IPv6, the source can check the size of the packet and make the decision to fragment the packet or not.
- When a router receives the packet, it can check the size of the packet and drop it if the size is larger than allowed by the MTU of the network ahead.
- The router then sends a packet-too-big ICMPv6 error message to inform the source.

iv) 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.
- 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, destination option, source routing, fragmentation, authentication and encrypted security payload.



Hop-by-Hop Option

- Is used when the source needs to pass information to all routers visited by the datagram.
- For eg., perhaps routers must be informed about certain management, debugging, control functions or the length of the datagram is more than the usual 65,535 bytes, routers must have this information.
- So far, only three hop-by-hop options have been defined: Pad1, PadN, and jumbo payload.

Destination Option

- Is used when the source needs to pass information to the destination only.
- Intermediate routers are not permitted access to this information.
- So far, only the Pad1 and PadN options have been defined.

Source Routing

- Combines the concepts of the strict source route and the loose source route options of IPv4.

Fragmentation

- 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.
- If the source does not use a Path MTU Discovery technique, it fragments the datagram to a size of 1280 bytes or smaller.

Authentication

- The authentication extension header has a dual purpose: it validates the message sender and ensures the integrity of data.
- The former is needed so the receiver can be sure that a message is from the genuine sender and not from an imposter.
- The latter is needed to check that the data is not altered in transition by some hacker.

Encrypted Security Payload

- Is an extension that provides confidentiality and guards against eavesdropping.