Unit 5: Network Layer [10 Hrs.]

5.1 Network Layer and its Functions

5.2 IPV4 Address and its Headers, IPv4 Classes

5.3 Private IP vs Public IP

5.4 Subnetting, Subnet Mask, FLSM, VLSM

5.5 Case Study

5.6 Issues with IPv4

5.7 Overview of IPv6 and its header format

5.8 Transition from IPv4 to IPv6

5.9 Routing: Adaptive and Non-Adaptive Routing, Distance Vector and Link State Routing

5.10 Famous Routing Protocols: RIP, OSPF, EIGRP, BGP

5.11 Ping(Lab Related), ICMP and NATing

5.1 Network Layer and its Functions

The Network Layer is the 5th Layer from the top and the 3rd layer from the Bottom of the OSI Model. It is one of the most important layers which plays a key role in data transmission. The main job of this layer is to maintain the quality of the data and pass and transmit it from its source to its destination. It also handles routing, which means that it chooses the best path to transmit the data from the source to its destination, not just transmitting the packet. There are several important protocols that work in this layer.
Data is transmitted in the form of packets via various logical network pathways between various devices. It offers routes for data packet transfers across the network. The network layer is also responsible for organizing and controlling the available paths for data transfer.

Functions of Network Layer

Assigning Logical Address: It provides unique IP addresses to devices for identification and communication across networks.

Packetizing: It encapsulates data into packets for efficient transmission.

Host-to-Host Delivery: It ensures data is delivered from the sender to the intended receiver across networks.

Forwarding: It is the process of moving packets from the input to the appropriate output interface in a router, based on the destination address.

Fragmentation and Reassembly: It splits large packets into smaller fragments for transmission and reassembles them at the destination.

Logical Subnetting: It divides larger networks into smaller subnetworks for better management and routing efficiency.

Network Address Translation (NAT): Maps private IP addresses to a public IP for internet access, conserving IPs and adding security.

Routing: It determines the best path for packets to travel to their destination across multiple networks.

5.2 IPV4 Address and its Headers, IPv4 Classes

IPV4 Address

An IPv4 address is a unique number assigned to every device that connects to the internet or a computer network. It's like a home address for your computer, smartphone, or any other device, allowing it to communicate with other devices.

Format: An IPv4 address is written as four numbers separated by periods, like this: 192.168.1.1. Each number can range from 0 to 255.

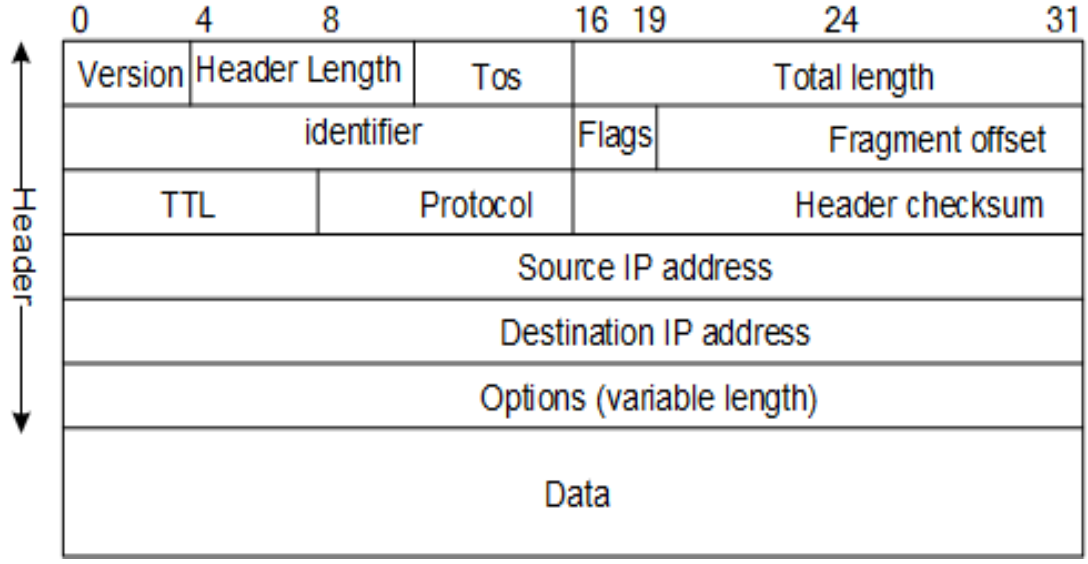
The IPv4 address is divided into two parts: NID (Network ID) = 8bit, and HID (Host ID) = 24bit. So there are 28 which is 256 total networks created and 224 which is 16M Host per network.

Purpose: The main purpose of an IPv4 address is to identify devices on a network and ensure that data sent from one device reaches the correct destination.

Example: When you type a website address into your browser, your device uses the IPv4 address to find and connect to the server where the website is hosted.

IPV4 Headers

Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.



IPv4 Datagram Header

VERSION: Version of the IP protocol (4 bits), which is 4 for IPv4

HLEN: IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.

Type of service: Low Delay, High Throughput, Reliability (8 bits)

Total Length: Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.

Identification: Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)

Flags: 3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)

Fragment Offset: Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.

Time to live: Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.

Protocol: Name of the protocol to which the data is to be passed (8 bits)

Header Checksum: 16 bits header checksum for checking errors in the datagram header

Source IP address: 32 bits IP address of the sender

Destination IP address: 32 bits IP address of the receiver

Option: Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.

IPV4 Classes

The 32-bit IP address is divided into five sub-classes. These are given below:

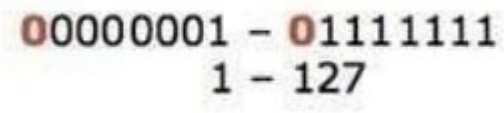
- Class A
- Class B
- Class C
- Class D
- Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determines the classes of the IP address.

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns an IP address to each device that is connected to its network.

1. Class A Address

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.



Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.
Class A IP address format is thus: 0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7) and 16777214 hosts (2^24-2).
Class A network IDs were assigned to networks with a very large number of hosts. Out of a total of 128 possible classes A networks, there are 126 networks and 16,777,214 hosts per network.

2. Class B Address
An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.

10000000 – 10111111
128 – 191

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.
Class B IP address format is: 10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH
Class B has 16384 (2^14) Network addresses and 65534 (2^16-2) Host addresses. Class B network IDs were assigned to medium to large-sized networks.

3. Class C Address
The first octet of Class C IP address has its first 3 bits set to 110, that is:

11000000 – 11011111
192 – 223

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.
Class C gives 2097152 (2^21) Network addresses and 254 (2^8-2) Host addresses.
Class C IP address format is: 110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH
Class C addresses were assigned to small networks.

5.3 Private IP vs Public IP

Public IP Address

Public IP address is assigned to every computer that connects to the Internet where each IP is unique. The Public IP Address of a system is the IP address that is used to communicate outside the network. A public IP address is basically assigned by the ISP (Internet Service Provider).

Public IP Address is basically of two types:

Dynamic IP Address: Dynamic IP Address are addresses that change over time. After establishing a connection of a smartphone or computer with the Internet, ISP provides an IP Address to the device, these random addresses are called Dynamic IP Address.

Static IP Address: Static IP Address are those addresses that do not change with time. These are stated as permanent internet addresses. Mostly these are used by the DNS (Domain Name System) Servers.

Private IP Address

The Private IP Address of a system is the IP address that is used to communicate within the same network. Using private IP data or information can be sent or received within the same network. The router basically assigns these types of addresses to the device. Unique private IP Addresses are provided to each and every device that is present on the network. These things make Private IP Addresses more secure than Public IP Addresses.

5.4 Subnetting, Subnet Mask, FLSM, VLSM

Subnetting

Subnetting is the process of dividing a large network into smaller networks called "subnets. A subnet is like a smaller group within a large network. It is a way to split a large network into smaller networks so that devices present in one network can transmit data more easily.

Subnet mask

The 32-bit IP address contains information about the host and its network. It is very necessary to distinguish both. For this, routers use Subnet Mask, which is as long as the size of the network address in the IP address. Subnet Mask is also 32 bits long. If the IP address in binary is ANDed with its Subnet Mask, the result yields the Network address. For example, say the IP Address is 192.168.1.152 and the Subnet Mask is 255.255.255.0 then.
This way the Subnet Mask helps extract the Network ID and the Host from an IP Address. It can be identified now that 192.168.1.0 is the Network number and 192.168.1.152 is the host on that network.

Address Class	Bits for Subnet Mask	Subnet Mask	Network Prefix
Class A	11111111 00000000 00000000 00000000	255.0.0.0	/8
Class B	11111111 11111111 00000000 00000000	255.255.0.0	/16
Class C	11111111 11111111 11111111 00000000	255.255.255.255	/32

CIDR Notation: A Simplified Approach to Subnetting
Instead of using a long subnet mask (e.g., 255.255.255.0), CIDR uses a simple format like /24. The number after the slash (/n) represents the number of bits used for the network portion of the IP address.

FLSM (Fixed Length Subnet Masking) is a subnetting technique where all subnets have the same number of IP addresses. It means the subnet mask is the same for every subnet, and each subnet supports the same number of hosts.

This method is easy to calculate and manage because each subnet is of equal size, but it may waste IP addresses if all subnets do not need the same number of hosts.

For example, suppose you have a network with the IP address 192.168.1.0 and you want to create 4 subnets using FLSM.

The original network is a Class C network with a default subnet mask of 255.255.255.0, which means there are 256 IP addresses in total (from 0 to 255). To divide this into 4 equal subnets, you borrow 2 bits from the host part because 2 bits can create 4 subnets (2^2 = 4).

New subnet mask becomes 255.255.255.192 or /26

Each subnet will have 64 IP addresses

So the 4 subnets will be:
192.168.1.0 to 192.168.1.63
192.168.1.64 to 192.168.1.127
192.168.1.128 to 192.168.1.191
192.168.1.192 to 192.168.1.255

In this case, each subnet has 64 IP addresses, even if one subnet needs only 10 hosts. The remaining addresses are unused, leading to wastage.

VLSM (Variable Length Subnet Masking)

Variable Length Subnet Masking (VLSM) is a way of further subnetting a subnet. Using Variable Length Subnet Masking (VLSM) we can allocate IPv4 addresses to the subnets by the exact need.
Variable Length Subnet Masking (VLSM) allows us to use more than one subnet mask within the same network address space.

For example, an administrator have 192.168.1.0/24 network. He has three different departments with different number of hosts. Sales department has 100 computers, Purchase department has 50 computers, Accounts has 25 computers and Management has 5 computers. In CIDR, the subnets are of fixed size. Using the same methodology the administrator cannot fulfill all the requirements of the network.

The following procedure shows how VLSM can be used in order to allocate department-wise IP addresses as mentioned in the example.

Step – 1
Make a list of Subnets possible.

Subnet Mask	Slash Notation	Hosts/Subnet
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2

Step - 2
Sort the requirements of IPs in descending order (Highest to Lowest).
Sales 100
Purchase 50
Accounts 25
Management 5

Step – 3
Allocate the highest range of IPs to the highest requirement, so let's assign 192.168.1.0 /25 (255.255.255.128) to the Sales department. This IP subnet with Network number 192.168.1.0 has 126 valid Host IP addresses which satisfy the requirement of the Sales department. The subnet mask used for this subnet has 10000000 as the last octet.

Step - 4
Allocate the next highest range, so let's assign 192.168.1.128 /26 (255.255.255.192) to the Purchase department. This IP subnet with Network number 192.168.1.128 has 62 valid Host IP Addresses which can be easily assigned to all the PCs of the Purchase department. The subnet mask used has 11000000 in the last octet.

Step – 5
Allocate the next highest range, i.e. Accounts. The requirement of 25 IPs can be fulfilled with 192.168.1.192 /27 (255.255.255.224) IP subnet, which contains 30 valid host IPs. The network number of Accounts department will be 192.168.1.192. The last octet of subnet mask is 11100000.

Step - 6
Allocate the next highest range to Management. The Management department contains only 5 computers. The subnet 192.168.1.224 /29 with the Mask 255.255.255.248 has exactly 6

valid host IP addresses. So this can be assigned to Management. The last octet of the subnet mask will contain 11111000.

By using VLSM, the administrators can subnet the IP subnet in such a way that least number of IP addresses are wasted. Even after assigning IPs to every department, the administrator, in this example, is still left with plenty of IP addresses which were not possible if the administrator has used CIDR.

5.5 Case Study

q1. Calculate the number of sub network and total no of host in a sub network for IP address 192.18.18.0/27. Also calculate the subnet mask, network address, Broadcast addresses and usable host range in each sub network.
Solution
The given IP- address is: 192.18.18.0/27

Therefore the subnet mask is: 11111111.11111111.11111111.11100000
That is: 255.255.255.224

Number of Host bits used in Network (N) = 3
Remaining Host bits (H) = 5

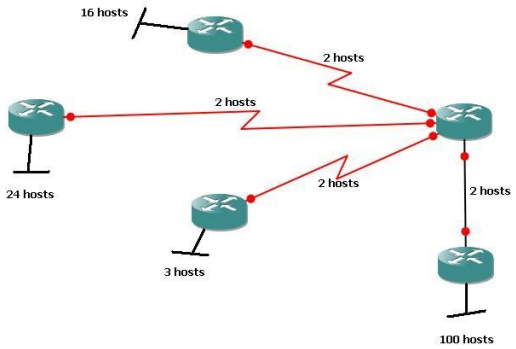
Total Subnets = 2^N = 2^3 = 8
Total Hosts = 2^H = 2^5 = 32

Valid Hosts per subnet = 32-2 = 30
Total no. of valid host over all subnet = 30 x 8 = 240
Block Size = 256 – Subnet mask = 256 – 224 = 32

The Subnet-ID, Host- IPs and Broadcast addresses of each subnet is calculated below.

S.N.	Subnet-ID	Host IP Range	Broadcast Address
1	192.18.18.0	192.18.18.1 →192.18.18.30	192.18.18.31
2	192.18.18.32	192.18.18.33 →192.18.18.62	192.18.18.63
3	192.18.18.64	192.18.18.63 →192.18.18.94	192.18.18.95
4	192.18.18.96	192.18.18.95 →192.18.18.126	192.18.18.127
5	192.18.18.128	192.18.18.129 →192.18.18.158	192.18.18.159
6	192.18.18.160	192.18.18.161 →192.18.18.190	192.18.18.191
7	192.18.18.192	192.18.18.193 →192.18.18.222	192.18.18.223
8	192.18.18.224	192.18.18.225 →192.18.18.254	192.18.18.255

Q2. Available Subnet – 24.23.5.0/24



We have to start from the biggest subnet

We have biggest subnet of 100 hosts

2x2x2x2x2x2x2 = 128 -2 = 126 hosts in a subnet

11111111.11111111.11111111.10000000

Subnet Mask for 100 hosts subnet is 255.255.255.128

Sunbet range - 24.23.5.0 - 24.23.5.127

Remaining IP range - 24.23.5.128 - 24.23.5.255

Next biggest subnet has 24 hosts

2x2x2x2x2 = 32 -2 = 30 hosts in a subnet

11111111.11111111.11111111.11100000

Subnet Mask for 30 hosts subnet is 255.255.255.224

Sunbet range - 24.23.5.128 - 24.23.5.159

Remaining IP Range - 24.23.5.160 - 24.23.5.255

Next biggest subnet has 16 hosts

2x2x2x2x2 = 32 -2 = 30 hosts in a subnet

11111111.11111111.11111111.11100000

Subnet Mask for 16 hosts subnet is 255.255.255.224

Sunbet range - 24.23.5.160 - 24.23.5.191

Remaining IP Range - 24.23.5.192 - 24.23.5.255

Next biggest subnet has 3 hosts

2x2x2= 8 -2 = 6 hosts in a subnet

11111111.11111111.11111111.111110 00

Subnet Mask for 3 hosts subnet is 255.255.255.248

Sunbet range - 24.23.5.192 - 24.23.5.199

Remaining IP Range - 24.23.5.200 - 24.23.5.255

Next four subnets has 2 hosts each

2x2 = 4 -2 = 2 hosts in a subnet

11111111.11111111.11111111.111111 00

Subnet Mask for 2 hosts subnet is 255.255.255.252

Sunbet range - 24.23.5.200 - 24.23.5.203

24.23.5.204 - 24.23.5.207

24.23.5.208 - 24.23.5.211

24.23.5.212 - 24.23.5.215

We still have remaining ip range from 24.23.5.216 - 24.23.5.255

You are given the network block:
192.168.1.0/24

You have the following departments that need IPs:

Department	No. of Hosts		
Admin	60	HR	30
Sales	14		
Accounts	7	Director	2

Task:
Using VLSM, divide the network and assign IP ranges to each department with:

Subnet Address Subnet Mask Broadcast Address First & Last Host

List departments in decreasing host order:
Add 2 extra for network & broadcast per subnet.

Department	Needed IPs	Next Power of 2
Admin	60	64 → /26
HR	30	32 → /27
Sales	14	16 → /28
Accounts	7	8 → /29
Director	2	4 → /30

Start subnetting from the base IP (192.168.1.0)

➤ Admin (/26 = 255.255.255.192)

Subnet: 192.168.1.0/26

Hosts: 62 usable

Range: 192.168.1.1 – 192.168.1.62

Broadcast: 192.168.1.63

➤ HR (/27 = 255.255.255.224)

Subnet: 192.168.1.64/27

Hosts: 30 usable

Range: 192.168.1.65 – 192.168.1.94

Broadcast: 192.168.1.95

➤ Sales (/28 = 255.255.255.240)

Subnet: 192.168.1.96/28

Hosts: 14 usable

Range: 192.168.1.97 – 192.168.1.110

Broadcast: 192.168.1.111

➤ Accounts (/29 = 255.255.255.248)

Subnet: 192.168.1.112/29

Hosts: 6 usable

Range: 192.168.1.113 – 192.168.1.118

Broadcast: 192.168.1.119

➤ Director (/30 = 255.255.255.252)

Subnet: 192.168.1.120/30

Hosts: 2 usable

Range: 192.168.1.121 – 192.168.1.122

Broadcast: 192.168.1.123

Unused IPs (optional):

Remaining from 192.168.1.124 – 192.168.1.255 → for future use.

5.6 Issues with IPv4

The main issues with IPv4 are its limited address space, leading to exhaustion and a growing reliance on workarounds like NAT, security vulnerabilities due to its lack of built-in security features, and inefficiencies in routing and configuration.

5.7 Overview of IPv6 and its header format

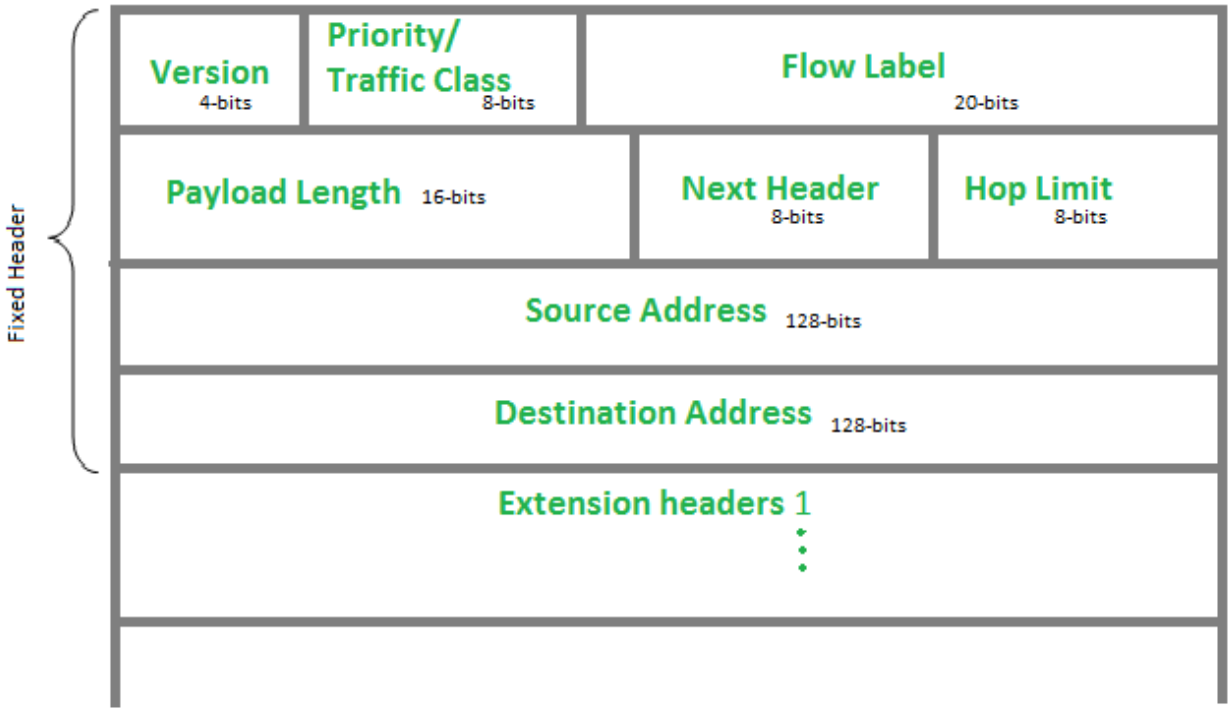
The Internet Protocol version 6, or IPv6, is the latest version of the Internet Protocol (IP), which is the system used for identifying and locating computers on the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the problem of IPv4 exhaustion. IPv6 is a 128-bit address having an address space of 2^128, which is way bigger than IPv4. IPv6 uses a Hexa-Decimal format separated by a colon (:).

Components in IPv6 Address Format

There are 8 groups and each group represents 2 Bytes (16-bits).
Each Hex-Digit is of 4 bits (1 nibble)
Delimiter used - colon (:)

IPV6 Header

The IPv6 header is the first part of an IPv6 packet, containing essential information for routing and delivering the packet across networks.



IPv6 fixed header is 40 bytes long and contains the following information.

1 Version (4-bits): It represents the version of Internet Protocol, i.e. 0110.

2 Traffic Class (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).

3 Flow Label (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re- ordering of data packets. It is designed for streaming/real-time media.

4 Payload Length (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.

5 Next Header (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.

6 Hop Limit (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.

7 Source Address (128-bits): This field indicates the address of originator of the packet.

8 Destination Address (128-bits): This field provides the address of intended recipient of the
packet.

5.8 Transition from IPv4 to IPv6

An IPv6 transition mechanism is a technology that facilitates the transitioning of the Internet from the Internet Protocol version 4 (IPv4) infrastructure in use since 1981 to the successor addressing and routing system of Internet Protocol Version 6 (IPv6). As IPv4 and IPv6 networks are not directly interoperable, transition technologies are designed to permit hosts on either network type to communicate with any other host.

Special methods are defined to handle interoperability, including:

“Dual Stack” Devices: Routers and some other devices may be programmed with both IPv4 and IPv6 implementations to allow them to communicate with both types of hosts.

IPv4/IPv6 Translation: “Dual stack” devices may be designed to accept requests from IPv6 hosts, convert them to IPv4 datagrams, send the datagrams to the IPv4 destination and then process the return datagrams similarly.

IPv4 Tunneling of IPv6: IPv6 devices that don't have a path between them consisting entirely of IPv6-capable routers may be able to communicate by encapsulating IPv6 datagrams within IPv4. In essence, they would be using IPv6 on top of IPv4; two network layers. The encapsulated IPv4 datagrams would travel across conventional IPv4 routers.

5.9 Routing: Adaptive and Non-Adaptive Routing, Distance Vector and Link State Routing

Routing is the process of selecting best paths in a network. The main function of the network layer is routing packets from source to machine to the destination machine.

Adaptive Routing algorithm

An adaptive routing algorithm is also called a dynamic routing algorithm. In this algorithm, the routing decisions are made based on network traffic and topology. The parameters that are used in adaptive routing algorithms are distance, hop, estimated transit time and count.

The adaptive routing algorithm is of three types -

Centralized algorithm
Isolation algorithm
Distributed algorithm

What is a Non-Adaptive Routing algorithm?

The non-adaptive routing algorithm is also called a static routing algorithm. In a non-adaptive routing algorithm, the routing decisions are not made based on network traffic and topology. This algorithm is used by static routing. Non-adaptive routing algorithms are simple as compared to Adaptive routing algorithms in terms of complexity.

The non-adaptive routing algorithm is of two types -

Flooding
Random walks

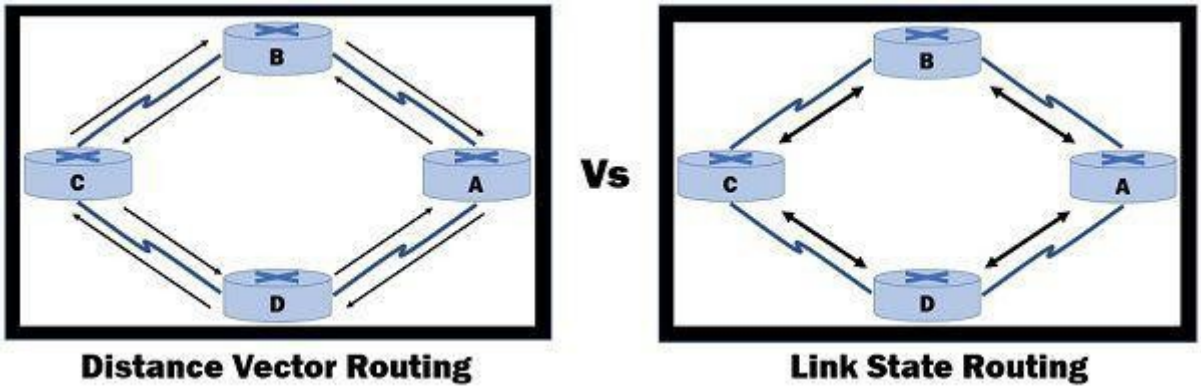
Distance Vector Routing and Link State Routing are two most used dynamic routing algorithms. They both are a part of Intradomain routing which refer to routing of devices within a same network.

Distance Vector Routing

Distance Vector Routing is an algorithm that is subject to change where a router calculates distances to every possible destination based on its immediate neighbors only, the router’s routing table is shared with routers that are directly connected, during regular intervals, this received information makes the routers update their tables while route computation uses Bellman-Ford algorithm most of the time, in spite of being relatively simple. However, Distance Vector Routing has some problems such as Count to Infinity or persistent routing loops.

Link State Routing

Link State Routing, as opposed to Distance Vector Routing, is a dynamic routing algorithm such that each router maintains knowledge of the entire network, instead of sharing information only with neighbors, routers flood their link state information across the entire network to make sure all routers have the same view of the network topology, Dijkstra's Algorithm and other Link State Routing algorithms are employed in order to compute shortest path to all destinations, it does not lead to persistent loop but it can result in more network traffic due to flooding link state information.



5.10 Famous Routing Protocols: RIP, OSPF, EIGRP, BGP

RIP (Routing Information Protocol):

Type: Distance-vector.
Metric: Primarily uses hop count.
Suitability: Best for small networks due to its simplicity but limited scalability (maximum 15 hops).
Updates: Sends periodic full routing table updates.

OSPF (Open Shortest Path First):

Type: Link-state.
Metric: Uses a cost metric based on bandwidth and delay, calculated using Dijkstra's SPF algorithm.
Suitability: Designed for large enterprise networks and service providers, offering scalability and efficient updates with features like areas for hierarchical routing.
Updates: Sends event-triggered Link State Advertisements (LSAs).

EIGRP (Enhanced Interior Gateway Routing Protocol):

Type: Advanced distance-vector or hybrid protocol.
Metric: Uses a composite metric based on bandwidth and delay, with features of both distance-vector and link-state protocols.
Suitability: Primarily used in Cisco-based networks, known for its fast convergence due to its DUAL algorithm.
Updates: Forms neighbor adjacencies and sends event-triggered updates.

BGP (Border Gateway Protocol):

Type: Path-vector protocol.
Metric: Focuses on path attributes like Autonomous System Numbers (ASNs) for routing between different autonomous systems.
Suitability: The de facto routing protocol for the internet, used for inter-domain routing between different organizations and ISPs.
Purpose: Manages routing between large, independent networks (Autonomous Systems) and offers extensive policy control.

5.11 Ping(Lab Related), ICMP and NATing

Ping is a computer network application used to test whether a particular host is reachable across an IP network. It is also used to self-test the network interface card of the computer or as a latency test. It works by sending ICMP “echo reply” packets to the target host and listening for ICMP “echo reply” replies.

ICMP (Internet Control Message Protocol)

ICMP is a network layer protocol used for sending error messages and diagnostics.

- Functions of ICMP:

  Report errors (e.g., destination unreachable)

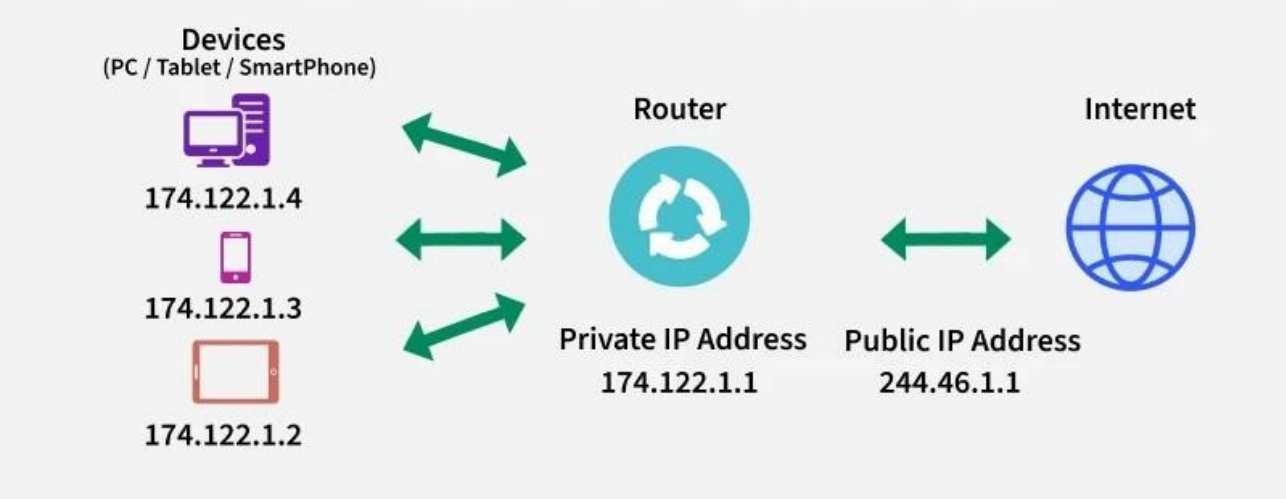
  Provide diagnostic tools (ping, traceroute)

  Send control messages

Type	Message	Description
0	Echo Reply	Ping response
8	Echo Request	Ping request
3	Destination Unreachable	Host/router unreachable
11	Time Exceeded	TTL expired (used in traceroute)

Network Address Translation(NAT)

Network Address Translation (NAT) is a process in which one or more local IP addresses are translated into one or more Global IP addresses and vice versa to provide Internet access to the local hosts. It also does the translation of port numbers, i.e., masks the port number of the host with another port number in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.



Types of Network Address Translation (NAT)

There are 3 ways to configure NAT:

Static NAT

In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global addresses. This is generally used for Web hosting. These are not used in organizations as there are many devices that will need Internet access and to provide Internet access, a public IP address is needed.

Suppose, if there are 3000 devices that need access to the Internet, the organization has to buy 3000 public addresses that will be very costly.

Dynamic NAT

In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP addresses. If the IP address of the pool is not free, then the packet will be

dropped as only a fixed number of private IP addresses can be translated to public addresses.

Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access the Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who want to access the Internet is fixed. This is also very costly as the organization has to buy many global IP addresses to make a pool.

Port Address Translation (PAT)

This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.