Sub: Computer Network & Security.

Unit III : Network Layer

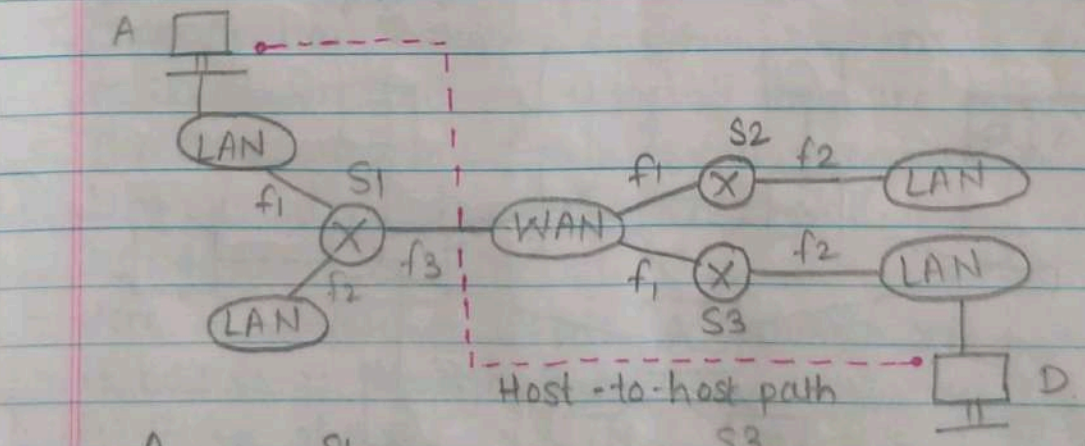
(Prof. Tejal Rane)

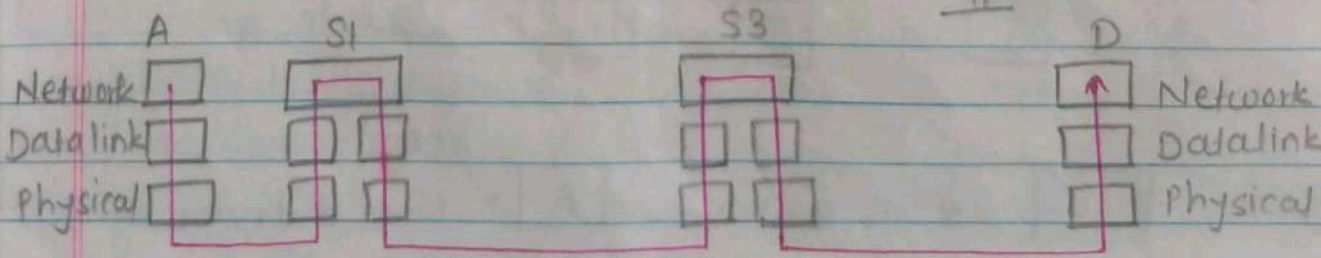
Network Layer:

- The network layer is the 5th layer from the top and the 3rd layer from the bottom of OSI Model.
- It plays a key role in data transmission and routing.
- Its main job is to deliver packets from source to destination while ensuring data quality.
- Data is transmitted in the form of packets through logical paths.
- This layer provides routing, addressing, and path selection across different networks.

Functions of Network Layer:

- Main function of Network Layer: The delivery of individual packets from the source host (node) to destination host (node) connected in different networks.





To carry out this function, the network layer needs the following:

→ **Internetworking**: connecting the hosts which are in different networks

→ **Packetizing**: dividing the message which is received from transport layer into packets.

→ **Logical addressing**: across different networks a logical address is required which is called Internet Protocol (IP) address.

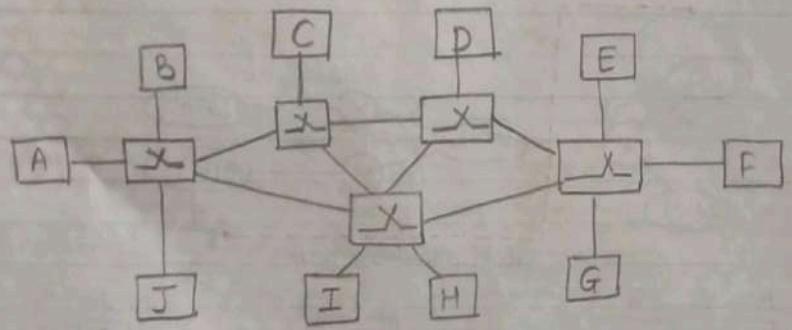
→ **Routing**: Protocols to decide to which path a packet has to be sent so that it reaches destination.

→ **Connection model**: connection-oriented and connectionless communication.

→ **Fragmenting**: dividing packets into fragments, if in between network does not allow big packets.

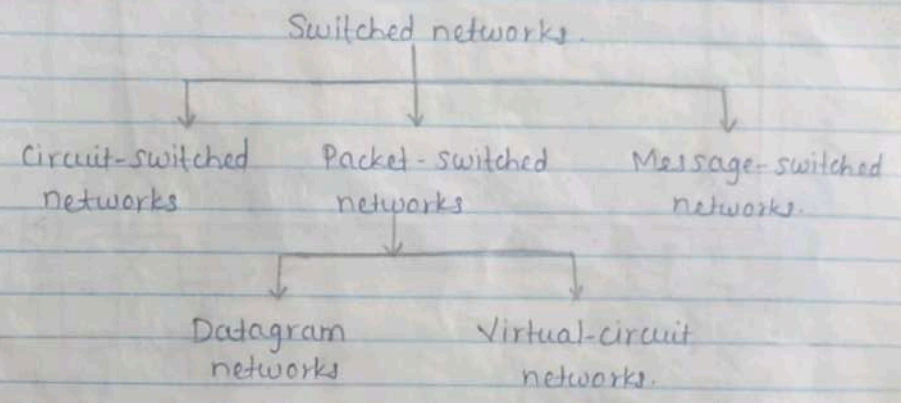
* **Switched Network**:

A switched network consists of interlinked nodes called switches, switches can create a temporary connection between two or more devices connected to it.



X is a switch A - is end device eg PC

§ **Switching Techniques**:

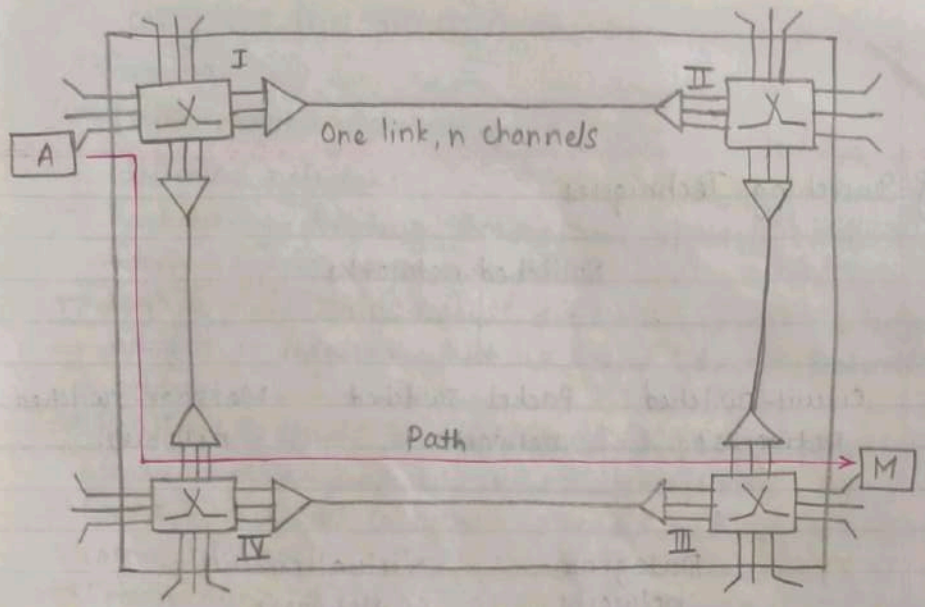


Classification of switching techniques.

(I) **Circuit Switching**:

- A circuit-switched network consists of a set of switches connected by physical links.
- A connection between any two stations is dedicated/reserved for that pair only till they are communicating.
- There is only one link between one pair of switches. Link is divided in to n channels (i.e. by multiplexing by using FDM or TDM).
- Here if station A wants to communicate with station M, it has to go through 3 phases:
  (1) Setup phase.
  (2) Data transfer phase
  (3) Teardown phase.

(Prof. Tejal Rane)



↳ Request of station A must be accepted by all switches in the path as well as M itself.

↳ In circuit switching, the resources need to be reserved during the setup phase such as switches in the path, channel between each switch, switch ports, etc.

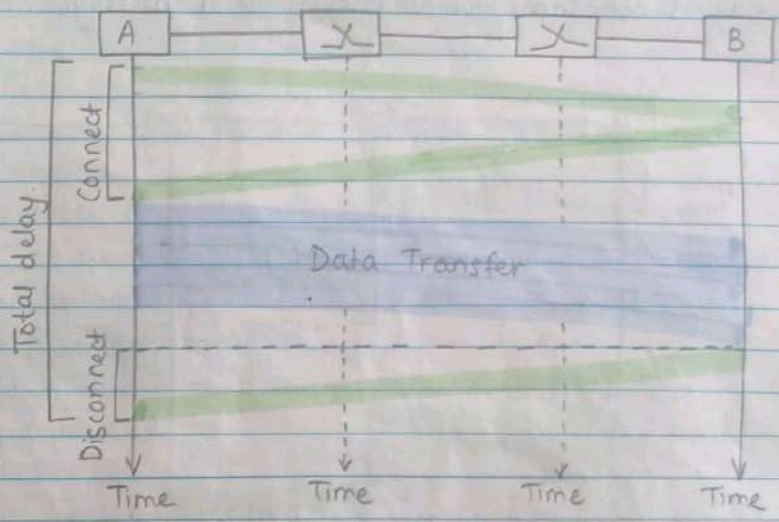
↳ The resources remain dedicated for the entire duration of data transfer until the teardown phase.

↳ Data transfer is not packetized but is continous flow with some periods of silence (eg. human conversation).

↳ Addressing is required only in the beginning i.e. during setup phase. No addressing required during data transfer and tear down.

↳ Efficiency: Less than packet switched. Resources allocated and reserved for a pair and cannot be shared by multiple pairs.

↳ Delay: It takes time for setup, but data transfer is fastest (as resources are reserved during setup).



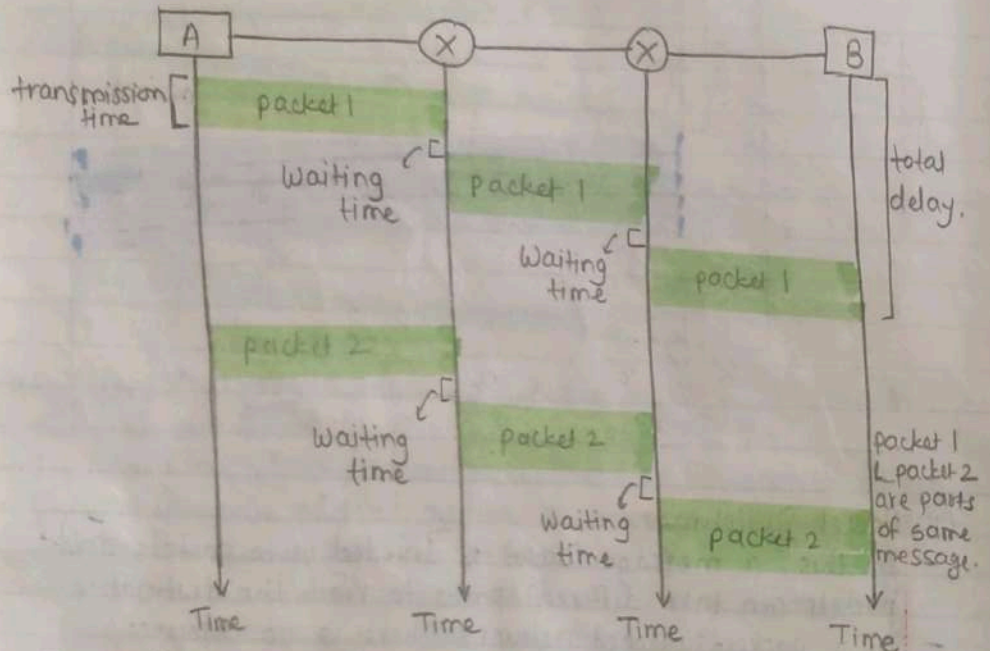
(II) Packet Switching:

- In this, a message (Data) is divided in to packets and packets can take different paths to reach the destination.
- In a packet-switched network, there is no resource reservation for communicating pairs. i.e. resources are allocated as available.
- Each packet is treated independently even if it is a part of the same message so each packet of the same message has same source and destination address.
- Packets may get lost, duplicated, damaged or out of order. It is duty of layers in end stations to take action accordingly.
- Efficiency: better than circuit switched. Resources allocated only when there are packets to be transmitted and can be shared

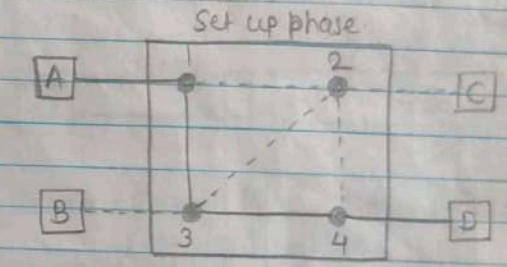
(Prof. Tejal Rane)

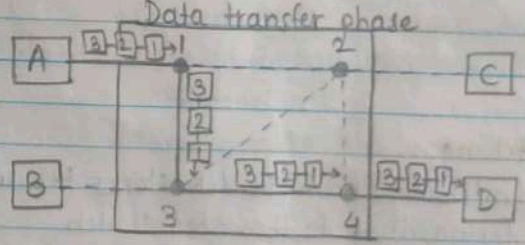
by multiple pairs.

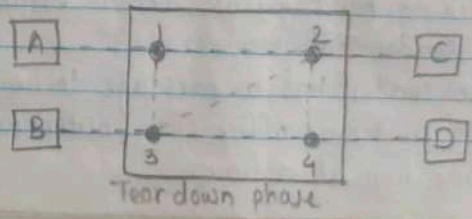
- Delay: Delay is greater than circuit switched network. There is no delay of setup and teardown phase, but at each switch, the packet has to wait in queue because of processing delay. Delay is not same for all packets of a message.



- Types of packet switching:
  - (i) Virtual Circuit network (Connection-Oriented Packet Switching):
    - ↳ A logical / virtual path is set up between sender and receiver before data transfer.
    - ↳ All packets follow the same predefined route.
    - ↳ Each connection is identified by a virtual circuit ID(VCI)
    - ↳ Packets have sequence numbers so that they arrive in order.
    - ↳ Phases:
      - (1) Setup Phase - Path established, address info exchanged.
      - (2) Data Transfer Phase - Packets transmitted with local info (length, timestamp, sequence).
      - (3) Tear Down phase - Virtual circuit is released.
    - ↳ Used in: X.25, Frame Relay, ATM, MPLS.
    - ↳ Advantages:
      - → Packets arrive in order.
      - → Less processing at each node (path already decided).
    - ↳ Disadvantages:
      - → Setup time required.
      - → If a switch fails, entire connection breaks.



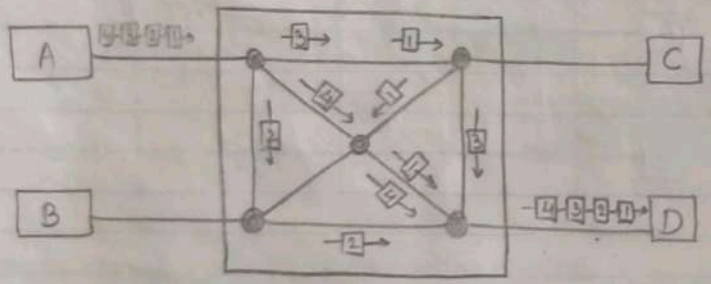




(Prof. Tejal Rane)

(ii) Datagram networks (Connectionless Packet Switching):

↳ Each packet is independent (no prior connection).
↳ Packet contains full address info (source, destination, port, control).
↳ Routing decisions made dynamically for each packet → may take different paths.
↳ Packets can arrive out of order or be lost.
↳ Reliability handled by end systems (eg. TCP).
↳ Used in: Internet (IP).
↳ Advantages:
→ No setup or teardown delay.
→ More robust (packets can reroute if a node fails).
↳ Disadvantages:
→ Packets may arrive out of order.
→ Requires extra overhead in packet headers.



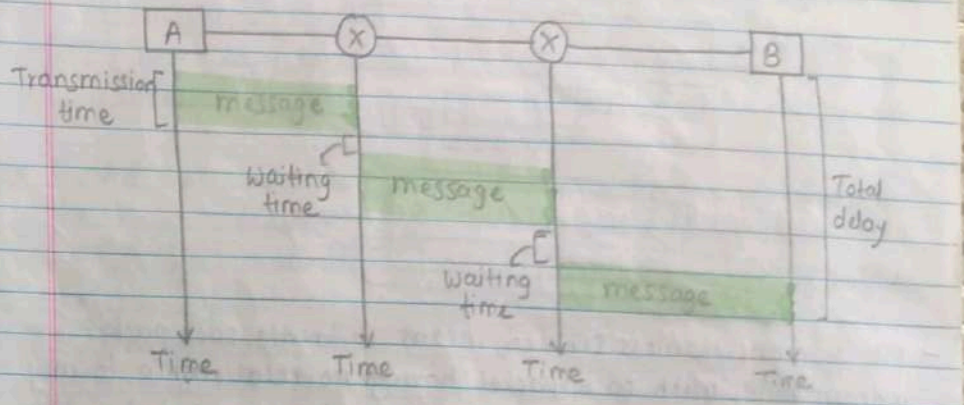
Datagram network.

(iii) Message Switching:

- In message switching, each switch stores the whole message and forwards it to the next switch.
- In message switching no physical path is established in advance between sender and receiver.
- Instead, when the sender has a message to be sent, it is stored in the first switching office (i.e., router) and then forwarded later, one hop at a time.

(Prof. Tejal Rane)

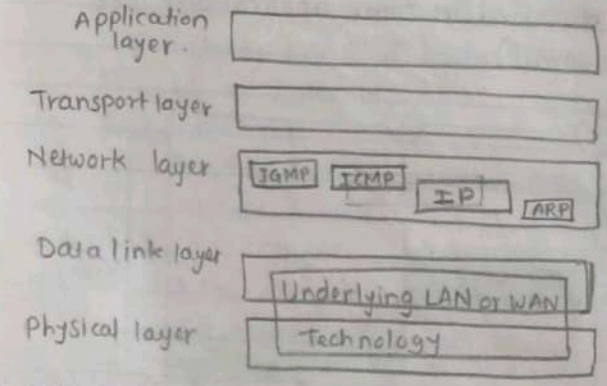
- Each message is received completely, then it is inspected for errors, and then retransmitted to next switch.
- Application: It is still used in some applications like electronic mail (e-mail).



	Circuit switching	Packet Switching	Message switching
	Entire message is transmitted.	Message is divided in to packets.	Entire message is transmitted.
Resource reservation	Resources (path)'s reserved for a particular pair	No resources are reserved.	No resources are reserved.
Phases	Three phases: Setup, data transfer, tear down	Only data transfer phase.	Only data transfer phase
Efficiency	Least.	High	High
Delay	Fastest data transfer	More delay	More delay.
Addressing	Required only during setup.	Each packet of same msg requires address of src & dest.	msg requires address of src & dest
Application	Telephone network	Internet	Email application

IP Protocol:

→ The IP Protocol is used at network layer. It is used for routing of packets from source to destination.
→ It is accompanied by other protocols such as IGMP, ICMP & ARP.



- IP is connectionless service, means it treats each packet independently, with each packet having no relationship to any other packet. Each packet has address of source & destination.
- IP is unreliable; means that IP packets can be corrupted, lost, arrive out of order, or delayed and may create congestion for the network. If reliability is important, IP must be paired with a reliable protocol such as TCP.
- IP has two versions based on address length.
  (1) IPv4 has 32 bit IP addresses for hosts & routers.
  (2) IPv6 has 128 bit IP addresses for hosts & routers.
- IPv6 can communicate with IPv4 hosts using techniques such as tunneling & header translation.

Classful IP Addressing:

Classful IP Addressing is an older method of dividing the IPv4 address space into fixed-size classes. It was in use from 1981 to 1993 until CIDR (Classless Inter-Domain Routing) replaced it.

↳ Addresses were divided into five classes (A, B, C, D, E) based on the first few bits.
↳ Each class had a default subnet mask, making configuration simple.
↳ It was easy to implement but led to wastage of IP addresses because of rigid block sizes.

- **Dotted Decimal Notation:**
  ↳ IPv4 addresses are written in dotted decimal notation (4 bytes separated by dots).
  ↳ Each byte strictly between 0-255 (both included) (8 bits → 2^8 values).
  ↳ No leading zeroes (eg. 054 is wrong, must be 54).
  ↳ Ex: 10000000 00001011 00000011 00011111
  128.11.3.31

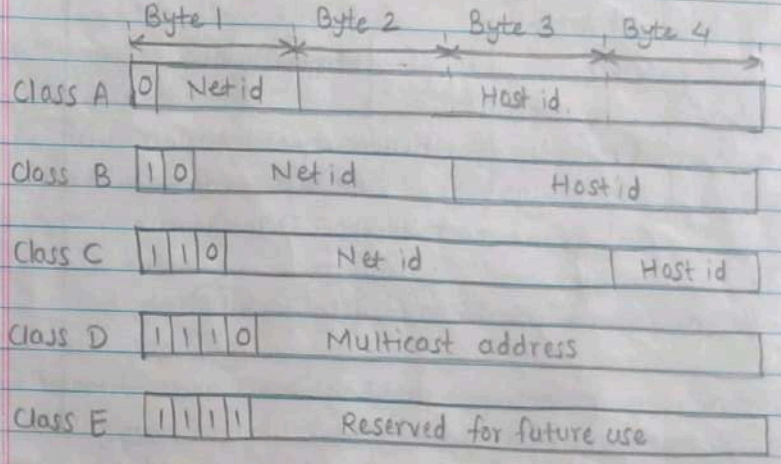
- **Hexadecimal notation:**
  01110101 00011101 10010101 11101010
  75 1D 95 EA
  0x751D95EA

- The address space of IPv4 is 2^{32} or 4,294,967,296.
- In classful addressing, the addresses are divided into five classes: A, B, C, D and E.
- Out of these, the classes A, B & C are used for networks, class D for groups messaging & class E for future applications.

(Prof. Tejal Rane)

- When first bit of IP address is '0', then it is class A address. Total number of class A networks/blocks are 127. Each class A network can have 16777216 addresses.
  - → Network ID: 8 bits.
  - → Host ID: 24 bits.
  - → Range: 0.0.0.0 – 127.255.255.255
  - → Default Subnet Mask: 255.0.0.0 → is like scissor which cuts IP into 2 parts – N/w ID & Host ID
- When first two bits of the address are '10', then it is class B address, total number of class B networks/blocks are 16384. Each class B network can have 65536 addresses.
  - → Network ID: 16 bits.
  - → Host ID: 16 bits.
  - → Range: 128.0.0.0 – 191.255.255.255
  - → Default Subnet Mask: 255.255.0.0
- When first three bits of the address are '110', then it is class C address, total number of class C networks/blocks are 2097152. Each class C network can have 256 addresses.
  - → Network ID: 24 bits.
  - → Host ID: 8 bits
  - → Range: 192.0.0.0 – 223.255.255.255
  - → Default Subnet Mask: 255.255.255.0
- When first four bits of the address are '1110', then it is class D address
  - → No Network ID/Host ID concept.
  - → Range: 224.0.0.0 – 239.255.255.255
  - → Purpose: Multicasting.
  - → No subnet mask.
- When first four bits of address are '1111', then it is class E address.
  - → Range: 240.0.0.0 – 255.255.255.255
  - → Purpose: Experimental/Research.
  - → No subnet mask.

Class	Number of networks/blocks	Size of network	Application
A	128	16,777,216 hosts	Unicast
B	16,384	65,536 hosts	Unicast
C	2,097,152	256 hosts	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

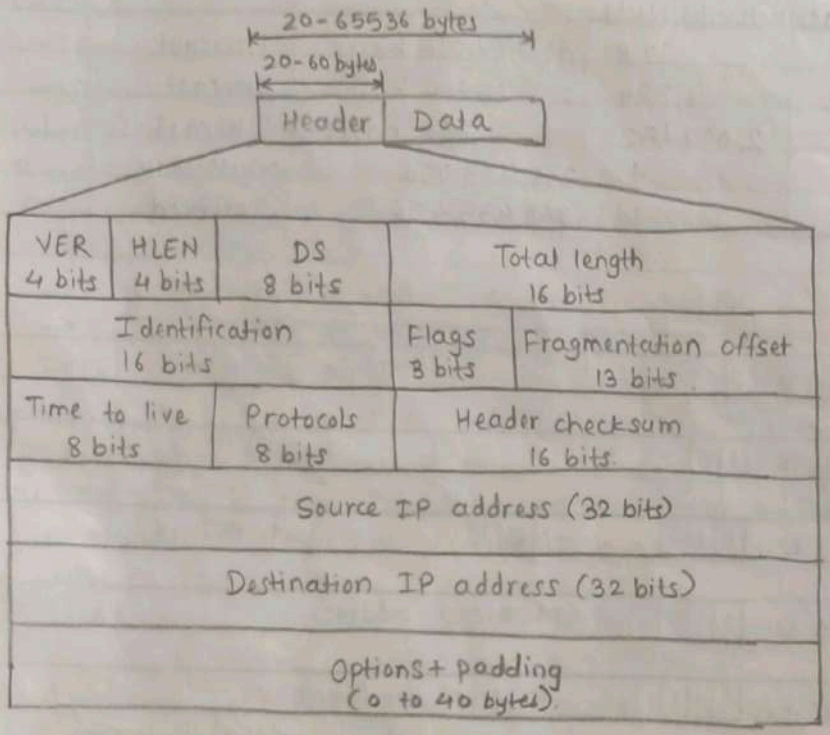


Limitations of Classful Addressing:
- Wastage of addresses (eg., small organization forced to take class B → wastes thousands of addresses)
- No flexibility of subnetting.
- Couldnot handle rapid internet growth so replaced by CIDR.

(Prof. Tejal Rane)

IPv4:

- Packets in the IPv4 layer are called datagrams. A datagram is a variable length packet consisting of two parts: Header and data.



- **Version (4 bits):** This field specifies the version of IP. For IPv4, the value is always 4. It ensures that the packet is interpreted using the correct format.
- **Header Length (HLEN) (4 bits):** Specifies the length of the IPv4 header in 32 bit (4-byte) words. The minimum value is 5 (20 bytes), and the maximum is 15 (60 bytes). It is needed because the header may include optional fields of variable length.
- **Type of Services (TOS)/Differentiated Services (8 bits):** Indicates the desired quality of service (QoS) for the datagram. It includes:
  - → Precedence bits (priority)
  - → Type of Service bits, which may request:
    - ↳ Minimized delay (e.g., for voice/video)
    - ↳ Maximized throughput (e.g., file transfers)
    - ↳ Maximized reliability (e.g., network management)
    - ↳ Minimized cost (e.g., background updates)
- **Total Length (16 bits):** Defines the total size of the IP datagram in bytes, including the header and data.
  - → Minimum: 20 bytes (header only).
  - → Maximum: 65,535 bytes.

  This helps receivers identify how much of the packet is valid data, especially in protocols like Ethernet that may add padding.
- **Identification (16 bits):** Used during fragmentation. If a datagram is split into multiple fragments, all fragments share the same identification value to allow reassembly at the destination.
- **Flags (3 bits):** Controls and manages fragmentation. The 3 bits are:
  - → Reserved bit (unused).
  - → DF (Don't Fragment): Prevents fragmentation.
  - → MF (More Fragments): Indicates more fragments follow.
- **Fragment Offset (13 bits):** Indicates the position of the fragment in the original datagram, in units of 8 bytes. It

(Prof. Tejal Rane)

helps in reassembling the datagram correctly at the destination.

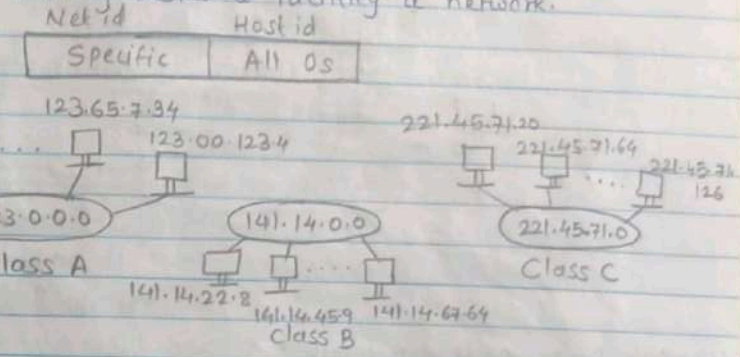
- **Time To Live (TTL) (8 bits):** Limits the lifespan of the datagram. It is decremented by 1 at each router hop. If it reaches zero, the packet is discarded. This prevents infinite looping in case of routing errors.
- **Protocol (8 bits):** Specifies the higher-level protocol that should receive the data at the destination.
  Ex: 1 - ICMP, 6 - TCP, 17 - UDP
  This tells the receiving host which protocol to pass the payload to.
- **Header Checksum (16 bits):** Used for error-checking the header only. The sender calculates a checksum before sending, and each router or receiver verifies it to detect any errors in the header during transmission.
- **Source IP Address (32 bits):** The unique IPv4 address of the sender. This remains unchanged as the datagram travels through the network.
- **Destination IP Address (32 bits):** The unique IPv4 address of the intended receiver. This is essential for routing and delivering the datagram to the correct host.
- **Options (Variable, Optional):** This field is used for additional features like security, record route, timestamp, etc. It is not commonly used and only present if HLEN > 5.
- **Padding (Variable, Optional):** Used to ensure the header ends on a 32-bit boundary. If options do not align the header to a multiple of 4 bytes, padding with zeros is added.

* **Special IPv4 addresses:**

In IPv4, some addresses are reserved for special purposes. These addresses are not assigned to normal hosts but are used for network identification, broadcasting, testing and special communication functions.

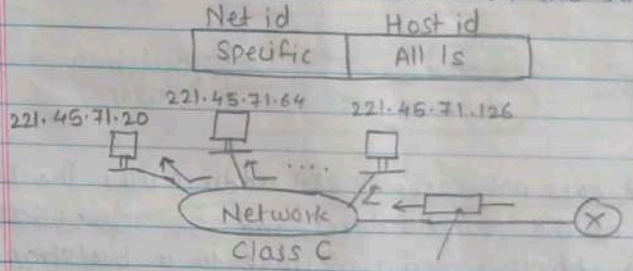
(1) **Network Address:**

- This is the first address of a network. All host bits are set to 0.
- It is used to represent the network itself and is mainly seen in routing tables to identify a network.



(2) **Broadcast Address:**

- This is the last address of a network. All host bits are set to 1. It is used to deliver data to all hosts within the same network at the same time.

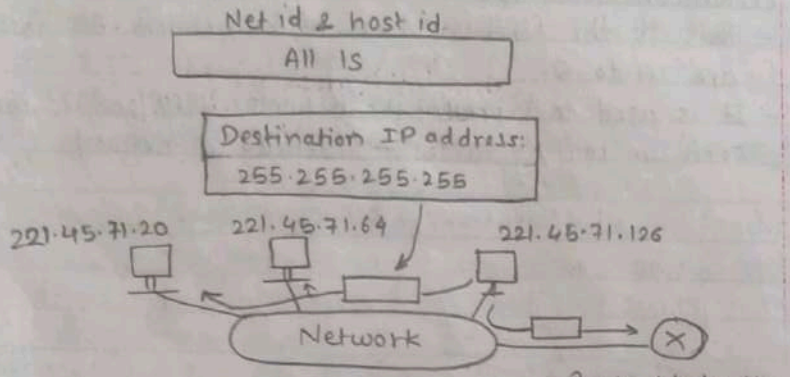


Destination IP address:
221.45.71.255
Host id: 255

(Prof. Tejal Rane)

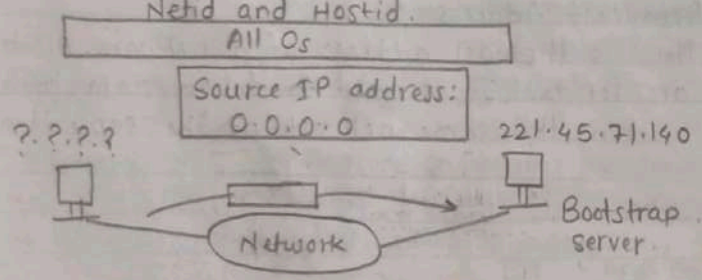
(3) Limited Broadcast Address:

- Used by a host in a network to send a packet to all hosts in the same network (broadcast). But it is blocked by router so it does not go outside of network.



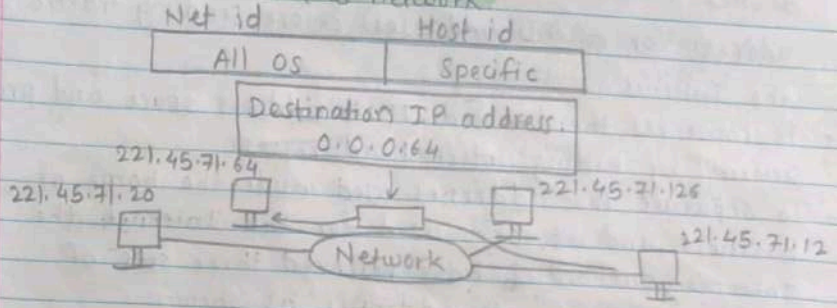
(4) This host on this network.

Used by DHCP server to assign IP to a host.



A host that does not know its IP address uses the IP address 0.0.0.0 as the source address and 255.255.255.255 as the destination address to send a message to a bootstrap server.

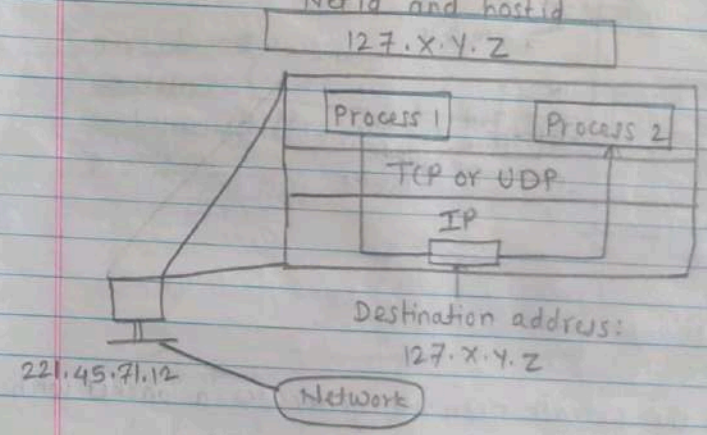
(5) specific host on this network:



This address is used by a router or host to send a message to a specific host on the same network.

(6) Loopback address:

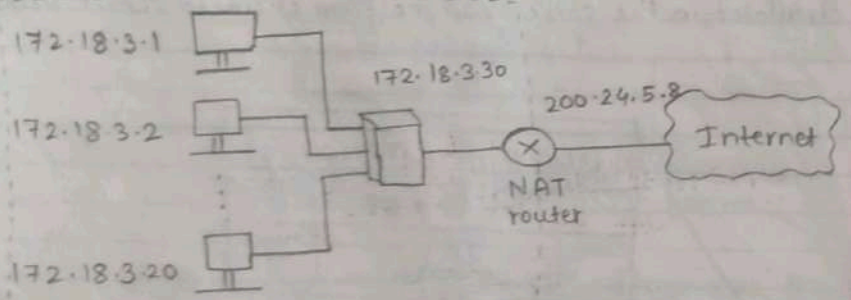
When two processes are in the same host. eg client & server program in same machine i.e. localhost.
This packet is not sent in the network by the host, but circulated in the same machine from client to server process.



(Prof. Tejal Rane)

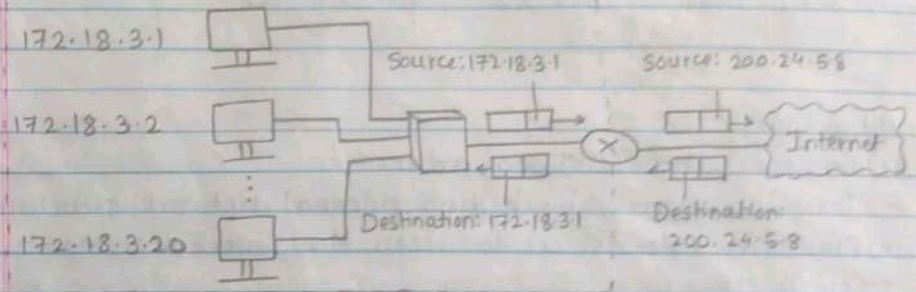
8 Network Address Translation (NAT):

- Network Address Translation (NAT) is a technique used by routers to translate private IP addresses of devices inside a local network into a single public IP address (or a few addresses) before sending traffic to the Internet.
- It conserves the limited IPv4 address space and provides security by hiding internal addresses.
- To separate the addresses used inside the home or business and the ones used for the Internet, the Internet authorities have reserved three sets of addresses as private addresses, as shown.
  - ↳ Class A: 10.0.0.0 – 10.255.255.255
  - ↳ Class B: 172.16.0.0 – 172.31.255.255
  - ↳ Class C: 192.168.0.0 – 192.168.255.255
- Any organization can use an address out of this set without permission from the Internet authorities. Since many organizations can use these addresses, they are not unique, so can't be used as public IP.



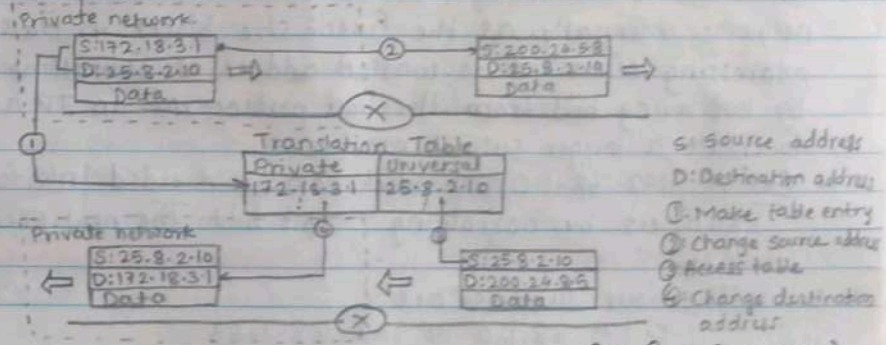
Site using private addresses

- NAT Process:
  (1) A host in the private network generates a packet with its private source IP address.
  (2) The packet reaches the NAT-enabled router.
  (3) The router replaces the private source IP with a public IP from its NAT table.
  (4) The packet is forwarded to the Internet.
  (5) When the response comes back, NAT router looks into its translation table, replaces the public IP with private IP, and delivers it to the correct internal host.



Site using private addresses

- Types of NAT:
  (1) Static NAT: One private IP is permanently mapped to one public IP.



(Prof. Teja Rane)

(2) Dynamic NAT: Private IPs are mapped to a pool of public IPs dynamically. Mapping is temporary.

(3) Port Address Translation (PAT)/overloading: Multiple private IPs mapped to a single public IP but with different port numbers. Most commonly used in home/office networks.

Private address	Private port	External address	External port	Transport protocol
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
⋮	⋮	⋮	⋮	⋮

- Advantages:
(1) Conserves public IPv4 addresses.
(2) Provides security by hiding internal network structure.
(3) Allows multiple devices to access the Internet using a single IP.

§ Subnetting:
- It is the process of dividing a large IP network into smaller, more manageable sub-networks (subnets). It was introduced to efficiently use IP addresses and organize networks internally, as the fixed-size blocks in classful addressing often led to wasted addresses. Subnetting works by borrowing bits from the host portion of an IP address to create a longer subnet mask.
- Ex: A 192.168.1.0/24 block can be divided into four subnets by borrowing 2 host bits. The new prefix is /26.
The four subnets are
↳ 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
Each subnet has 64 total addresses, with 62 being usable hosts.
- Advantages:
→ Efficient IP usage: Prevents address wastage.
→ Reduced broadcast traffic: Confines broadcasts to a single subnet.

§ Supernetting:
- Supernetting is the opposite of subnetting. It combines multiple smaller networks into a single, larger block. This was used when Class C networks were too small for an organization's needs. This process decreases the number of 1s in the mask (using a shorter prefix).
- Ex: Four contiguous Class C blocks (192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24) can be combined into a single supernetwork.
The combined network is 192.168.0.0/22 which provides 1024 addresses.
- Advantages:
→ Route Aggregation: Reduces the number of entries in routing tables.
→ Flexibility: Provides appropriately sized address blocks.

§ Classless Addressing (CIDR): Classless InterDomain Routing):
CIDR was introduced in 1993 to replace the rigid classful

(Prof. Tejal Rane)

system. It allocates addresses in variable-length blocks and uses prefix length (slash notation, /n) to specify network bits.

- CIDR Notation: x.y.z.t/n
- Block Size: Total addresses in a block are $2^{(32-n)}$
- Rules for Allocation: Blocks must be a power of 2, and the first address must be divisible by block size.

To solve numerical problems, use these formulas.

- Total Host Bits: h = 32 − CIDR Prefix Length
- Total Addresses (Block Size): 2^h
- Usable Hosts: $(2^h - 2)$

CIDR Prefix to Subnet Mask:

CIDR Prefix	SubNet Mask (Dotted Decimal)	Last Octet (Binary)
/24	255.255.255.0	00000000
/25	255.255.255.128	1000 0000
/26	255.255.255.192	1100 0000
/27	255.255.255.224	1110 0000
/28	255.255.255.240	11110000
/29	255.255.255.248	11111000
/30	255.255.255.252	11111100

Example: Q. A host was given the 192.168.2.64/25 IP address. Indicate:

(1) The subnet mask of the network in dotted-decimal notation.
(2) The network address to which the host belongs.
(3) The network broadcast address to which the host belongs.
(4) The total number of hosts available in the network.

Soln: The CIDR prefix is /25.
Network bits: 25
Host bits: 32 − 25 = 7

The /25 prefix corresponds to a subnet mask with 25 consecutive 1's
Dotted decimal: 255.255.255.128

The host bits are 7 ∴ Block size $2^7 = 128$
The valid networks are multiple of 128 in last octet
The possible networks are 192.168.2.0 and 192.168.2.128
The host IP 192.168.2.64 falls in range of first network (0 to 127).
∴ The network address is 192.168.2.0

The current network starts at 192.168.2.0
The next network starts at 192.168.2.128
The broadcast address is address immediately before the next network.
∴ The broadcast address is 192.168.2.127

Total addresses/block size = 128
Usable hosts = 128 − 2 = 126
∴ The total number of hosts available is 126.

(Prof. Tejal Rane)

§ IPv6 Addresses and Protocol:

- IPv4, with its 32-bit address, can provide around 4.3 billion addresses, which are now almost exhausted.
- To overcome limitations such as address depletion, lack of support for real-time traffic, and poor security, the Internet Engineering Task Force (IETF) developed IPv6 (Internet Protocol version 6), also known as IPng (Next Generation IP).
- IPv6 uses 128-bit addresses, providing an extremely large address space (2^{128} addresses).
- Structure:
  - ↳ IPv6 address = 128 bits = 16 bytes
  - ↳ Written in hexadecimal colon notation: divided into 8 groups, each of 16 bits (4 hex digits), separated by colons.

    Ex:

    Binary (128 bits) 1111111011110110 ... 1111111100000000
    Colon Hexadecimal FEF6:BA98:7654:3210:ADEF:BBFF:2922:FF00
- Abbreviations:
  - ↳ Leading zeros in each group can be omitted
    - → 0032 → 32
  - ↳ A continuous sequence of zero groups can be replaced by :: (only once per address).
  - ↳ Ex: FDEC:0074:0000:0000:0000:B0FF:0000:FFF0
    - → FDEC:74:0:0:0:B0FF:0:FFF0
    - → FDEC:74::B0FF:0:FFF0
- Address Space: The address space of IPv6 contains 2^{128} addresses = 340,282,366,920,938,463,374,607,431,768,211,456
- **Types of IPv6 Addresses:** IPv6 addresses are classified based on the prefix (starting bits). Main categories:

  (i) **Unicast Address:**
  - ↳ Identifies a single unique node on the network.
  - ↳ Packet delivered to exactly one destination.
  - ↳ Types:
    - → Provider-based unicast (commonly used; includes ISP, subscriber, subnet, and node identifiers).
    - → Geographic-based unicast (reserved for future use).

  (ii) **Multicast Address:**
  - ↳ Represents a group of nodes.
  - ↳ Packet sent to a multicast address is delivered to all members of the group.
  - ↳ Example: real-time video conferencing, live streaming.
  - ↳ Scope can be: node-local, link-local, site-local, or global.

  (iii) **Anycast Address:**
  - ↳ Assigned to a group of nodes, but a packet is delivered to the nearest node (shortest path).
  - ↳ Ex: Used for routing to the nearest DNS server or nearest ISP router.

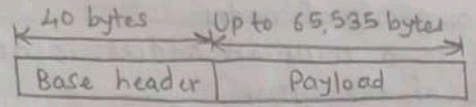
  (iv) **Reserved Addresses:**
  - ↳ Unspecified (0:0:0:0:0:0:0:0/::) → used when a host does not know its IP.
  - ↳ Loopback (::1) → host sends message to itself.
  - ↳ IPv4-compatible (::IPv4-address) → used during IPv4-IPv6 transition.
  - ↳ IPv4-mapped (::FFFF:IPv4-address) → allows IPv6 nodes to communicate with IPv4 nodes.

  (v) **Local Addresses:**
  - ↳ Used inside organizations, not routed on global Internet.
    - → Link-local (FE80::/10): communication within a

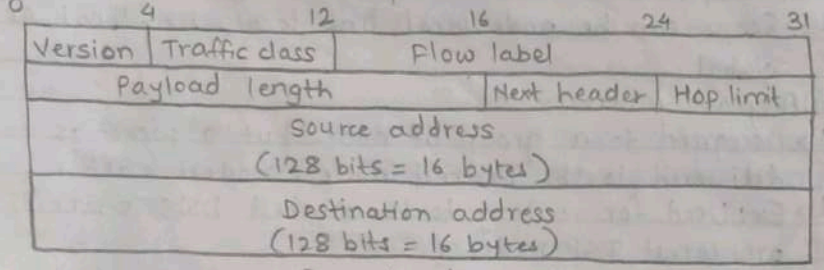
(Prof. Tejal Rane)

Single link (like LAN).
→ Site-local (FECO::/10): communication within a site (deprecated, replaced by unique local addresses).

- **IPv6 Packet Format:**
  ↳ An IPv6 packet consists of:
  (1) Base Header (fixed size of 40 bytes) - mandatory.
  (2) Extension Headers (optional, if needed)
  (3) Payload / Data - actual data from upper-layer protocols (TCP, UDP, etc.)



IPv6 packet



Base header

(i) **Version (4 bits):** Specifies the IP version. Value is always 6 for IPv6.
(ii) **Traffic class/ Priority (8 bits):**
- Defines the class or priority of the packet
- Used for Quality of Service (QoS) to differentiate delay-sensitive traffic (e.g., voice, video) from normal data.

(iii) **Flow Label (20 bits):**
- Identifies a sequence of packets (flow) that requires special handling, such as real-time streaming.
- Helps routers recognize and give consistent treatment to packets belonging to the same flow.

(iv) **Payload Length (16 bits):**
- Indicates the size of the payload (data + extension headers) in bytes.
- Maximum payload size is 65,535 bytes.

(v) **Next Header (8 bits):**
- Identifies the type of header immediately following the IPv6 base header.
- Ex: - 06 → TCP
  - 17 → UDP
  - Values may also indicate an extension header (eg. routing header, authentication header).

(vi) **Hop Limit (8 bits):**
- Similar to the TTL (Time-to-Live) field in IPv4.
- Indicates the maximum number of hops (routers) the packet can pass.
- Each router decreases the value by 1. When it reaches 0, the packet is discarded.

(vii) **Source Address (128 bits):** IPv6 address of the sender. Uniquely identifies the origin of the packet.

(viii) **Destination Address (128 bits):** IPv6 address of the final recipient. Uniquely identifies the target node.

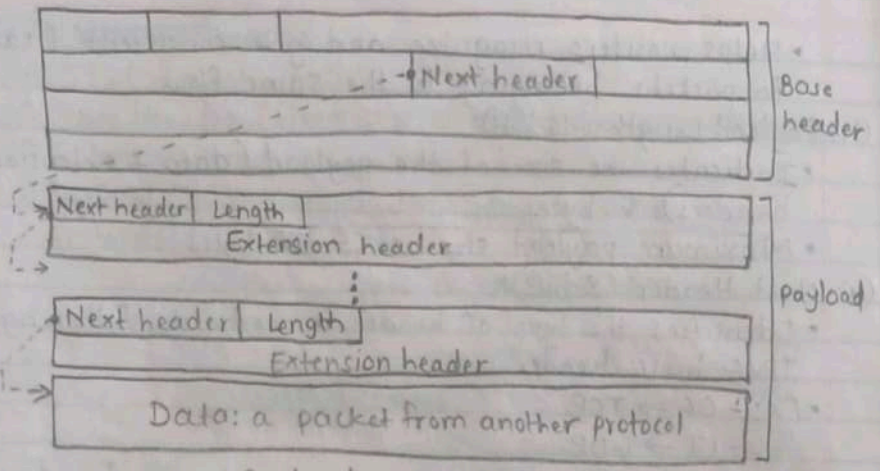
(ix) **Payload:** Compared to IPv4, the payload field in IPv6 has a different format.

- **IPv6 Extension Headers:**
- Extension headers provide additional functionalities such

(Prof. Tejal Rane)

as security, routing or fragmentation.

- They are placed after the base header and are processed in the order they appear.



Payload in an IPv6 datagram

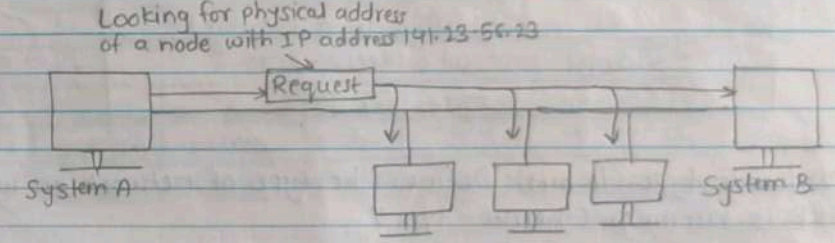
- Common extension headers include:
  (1) Hop-by-Hop Options: processed by every router along the path.
  (2) Routing Header: specifies intermediate nodes.
  (3) Fragment Header: used for fragmentation (done only at the source in IPv6).
  (4) Authentication Header (AH): provides authentication and integrity.
  (5) Encapsulating Security Payload (ESP): provides confidentiality and encryption.

Network Layer Protocols:

(I) Address Resolution Protocol (ARP)
(II) Reverse Address Resolution Protocol (RARP)
(III) Internet Control Message Protocol (ICMP)
(IV) Internet Group Management Protocol (IGMP)

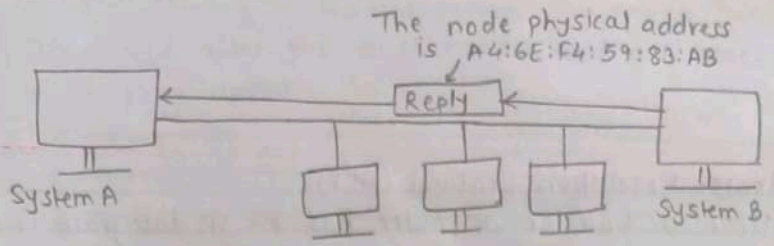
(I) Address Resolution Protocol (ARP):

- Anytime a host or a router has an IP datagram to send to another host or router, it has the logical (IP) address of the receiver.
- The logical (IP) address is obtained from the DNS if the sender is the host or it is found in a routing table if the sender is a router.
- But the IP datagram must be encapsulated in a frame to be able to pass through the physical network.
- This means that the sender needs the physical address of the receiver.
- The host or router sends an ARP query packet.
- The packet includes the physical and IP addresses of the sender and the IP address of the receiver.
- Because the sender does not know the physical address of the receiver, the query is broadcast over the network.



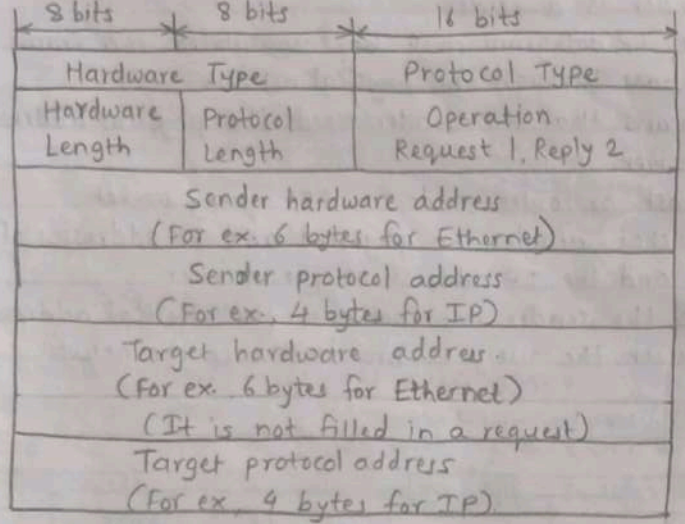
ARP request is broadcast.

(Prof. Tejal Rane)



ARP reply is unicast

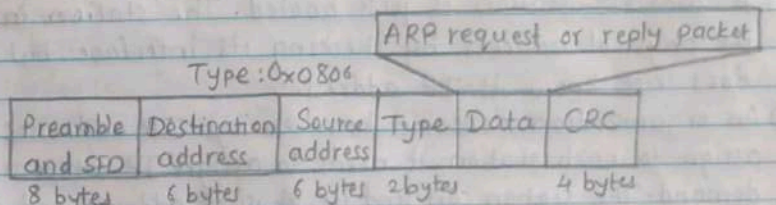
ARP Packet:



- **Hardware type: (16 bits)**: Defines the type of network on which ARP is running. Ethernet - type I.
- **Protocol type (16 bits)**: This field defines protocol. IPv4 - 0800H.
- **Hardware Length (8 bits)**: Defines length of physical address in bytes. (Ethernet - 6).
- **Protocol length (8 bits)**: Defines the length of logical address in bytes. (IPv4 - value is 4).
- **Operation (request or reply) (16 bits)**: Defines the type of packet. Packet types are ARP request (1) and ARP reply (2).
- **Sender hardware address**: This is a variable length field defining the physical address of the sender.
- **Sender protocol address**: This is a variable length field defining the logical address of the sender.
- **Target hardware address**: This is a variable length field defining the physical address of the target.
- **Target protocol address**: This is a variable length field defining the logical address of the target.

Encapsulation of ARP Packet:

- An ARP packet is encapsulated directly into a data link frame (Ethernet frame).
- In the Ethernet protocol, Type value 0x0806 indicates that the frame contains an ARP datagram/packet.



Operation:

1. The sender knows the IP address of the target.
2. IP asks ARP to create an ARP request message, filling in the sender physical address, the sender IP address, and the target IP address. The target physical address field

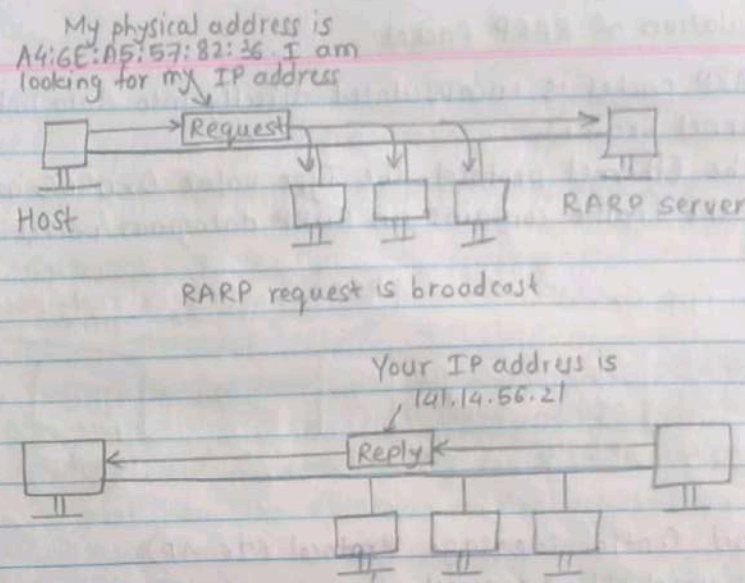
(Proof. Tejal Rane)

with 0s.

3. The message is passed to the DLL where it is encapsulated in a frame by using the physical address of the sender as source address and the physical broadcast address as the destination address.
4. Every host or router receives the frame. All machines except the one targeted drop the packet. The target machine recognizes its IP address.
5. The target machine replies with an ARP reply message that contains its physical address. The message is unicast.
6. The sender receives the reply message. It now knows the physical address of the target machine
7. The IP datagram, which carries data for the target machine, is now encapsulated in a frame and is unicast to the destination.

(II) Reverse Address Resolution Protocol

- There are occasions in which a host knows its physical address, but needs to know its logical address. This may happen in two cases:
  (1) A diskless station is just booted. The station can find its physical address by checking its interface, but it does not know its IP address.
  (2) An organization does not have enough IP addresses to assign to each station; it needs to assign IP addresses on demand. The station can send its physical address and ask for a short time lease.
- RARP is used for this purpose.
- The requesting machine must be running a RARP client program; the responding machine must be running a RARP server program.



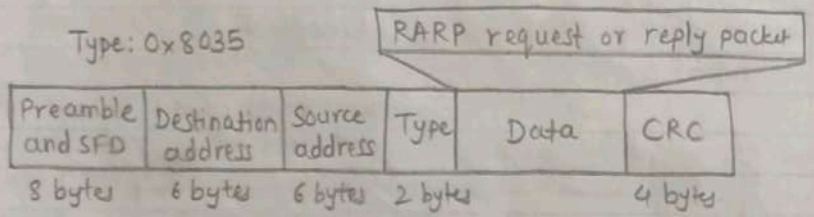
RARP Packet:

Hardware type		Protocol type
Hardware length	Protocol length	Operation Request 3, Reply 4
Sender hardware address (For ex. 6 bytes for Ethernet)		
Sender protocol address (For ex. 4 bytes for IP) (It is not filled for request)		
Target hardware address (For ex. 6 bytes for Ethernet) (It is not filled for request)		
Target protocol address (For ex. 4 bytes for IP) (It is not filled for request)		

(Prof. Tejal Rane)

Same as that of ARP except operation field (3 for RARP request and 4 for RARP reply).

- Encapsulation of RARP Packet:
  - ↳ An RARP packet is encapsulated directly into data link frame (Ethernet Frame).
  - ↳ In the Ethernet protocol, the Type value 0x0805 indicates that the frame contains an RARP datagram/packet.



(III) Internet Control Message Protocol (ICMP):

- IP is unreliable & connectionless i.e. no error reporting or correction.
- IP also lacks query/management features.
- ICMP was designed as a companion protocol to compensate these deficiencies.
- Encapsulated inside IP packets (Protocol field = 1).
- ICMP Message Types: There are two main categories:
  1. Error Reporting Messages
  2. Query Messages:

1. Error Reporting Messages:

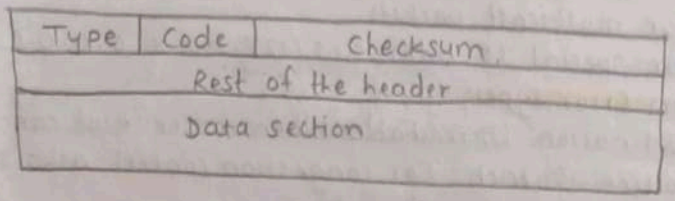
- ↳ Sent to the source host when a packet cannot be delivered.
- ↳ Never generated for following cases:
  - → In response to another ICMP error.
  - → For a fragmented datagram (except the first).
  - → For multicast packets.
  - → For special IP addresses (127.x.x.x, 0.0.0.0)
- ↳ Main Error Types:
  1. Destination Unreachable: When router/host cannot deliver.
  2. Source Quench: For congestion control; asks sender to slow down.
  3. Time Exceeded: When TTL field = 0, packet discarded.
  4. Parameter Problem: Invalid/missing field in IP header.
  5. Redirect: Router informs host about a better route.
     Ex: If Host A sends via Router R1 but R2 is a better next hop then R1 sends a Redirect message to host A. Host A then updates routing table.

2. Query Messages:

- ↳ Used for diagnostics and network management.
- ↳ Always occur in request-reply pairs.
- ↳ Main Query Types:
  1. Echo Request/Echo Reply: Checks if host is alive. used in PING Command.
  2. Timestamp Request/Reply: Measures round trip delay. Can synchronize clocks between two hosts.
  3. Address Mask Request/Reply: Helps a host discover its subnet mask.
  4. Router Solicitation/Advertisement: Hosts asks for nearby routers. Routers reply with their presence and preference level (default router selection).

(Prof. Tejal Rane)

- General ICMP Message Format:
  ↳ The message has an 8-byte header and a variable size data section.



  ↳ **Type:** Defines the type of message (error/query)
  ↳ **Code:** Specifies the reason for the particular message type
  ↳ **Checksum:** Similar to IP header checksum. It is calculated over entire ICMP message.
  ↳ The rest of the header is specific for each message type.
  ↳ **Data section:**
    → In error messages carries information for finding the original packet that had the error
    → In query messages carries extra information based on the type of query.

(IV) Internet Group Management Protocol (IGMP):

- Multicasting is one to many communication (eg. distance learning, live streaming, stock updates)
- IP supports multicast addressing
- IGMP is not routing protocol instead, it manages group membership.
- Used locally in LAN between hosts and multicast routers.
- Purpose
  ↳ Helps routers know which multicast groups have members on their LAN.
  ↳ Without IGMP, routers would need to flood all multicast packets that wastes bandwidth.
  ↳ With IGMP, routers keep membership lists and forward multicast packets only where needed.

- **IGMP message types:**
  ↳ IGMP messages are carried in bare IP Packets (Protocol=2)
  1. **Query Messages:**
     → Sent by a designated router.
     → General Query: asks all hosts about all groups.
     → Group Specific Query: check interest for one group
     → Group and Source Specific Query: interest in one group but only from specific sources
  2. **Membership Report:**
     → Sent by hosts/routers to join a group.
     → Sent twice (to prevent loss).
  3. **Leave Group Message:**
     → Sent by host/router when leaving a group.
     → Router then verifies with a query if other members still exist before removing group entry.

- **IGMP operation:**
  ↳ **Joining a group:**
    → A host process requests membership then host sends a membership report.

(Prof. Tejal Rane)

→ If host already subscribed, no new report is sent.

↳ Leaving a group:
→ Host sends leave report → router verifies if other member exists.
→ If none respond, router removes group.

↳ Query Router:
→ Only one router per LAN sends queries to avoid flooding.

- IGMP Message Format:

Type	Maximum response time	Checksum
Group address in membership and leave reports and special query; all 0s in general query		

↳ Type (8 bits):
→ General / Specific Query = 0x11
→ Membership Report = 0x16
→ Leave Group = 0x17

↳ Maximum Response Time: Time in which reply must be given.

↳ Checksum: For error detection.

↳ Group Address:
→ 0 for general queries.
→ Contains multicast group address for other messages.

8 Network Routing & Algorithms:

* Routing Table:

- A routing table is maintained by a host or router.
- It contains entries for destination to forward IP packets.
- Two types: Static Routing and Dynamic Routing.

1. Static Routing:

↳ Routing table entries are manually entered by the administrator.

↳ Does not update automatically when nlw changes occur.

↳ If there is a new route, link failure, or shutdown then administrator must manually modify.

↳ Advantages:
→ Simple to configure.
→ Useful in small nlws or for testing/troubleshooting.

↳ Disadvantages:
→ Not suitable for large or frequently changing nlws.
→ Manual updates are time-consuming and error-prone.

2. Dynamic Routing:

↳ Routing table is updated automatically using routing protocols (eg. RIP, OSPF, BGP).

↳ Whenever there is a link failure, shutdown, or change, routers exchange information and updates routers.

↳ Ensures efficient delivery of packets in large scale internetworks like the Internet.

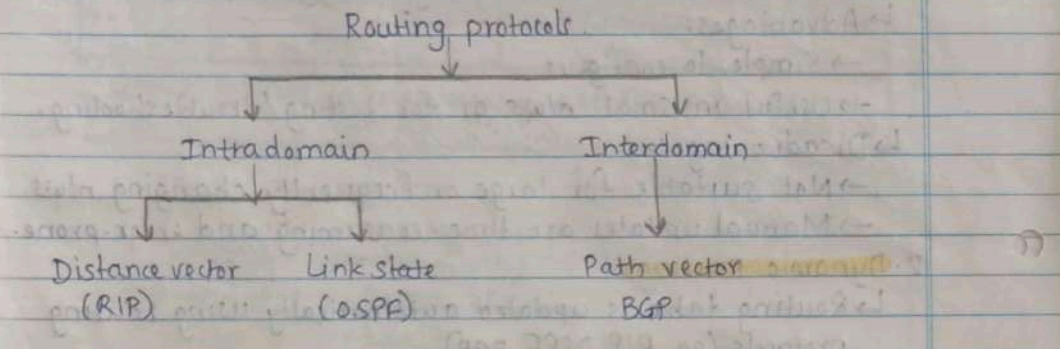
↳ Advantages:
→ Automatic updates which reduces admin effort.
→ Scales well for large, complex networks.
→ Adapts quickly to topology changes.

(Prof. Tejal Rane)

↳ Disadvantages:
→ More complex than static routing.
→ Requires processing power and bandwidth to exchange updates.

* Autonomous Systems (AS):

- An Autonomous System (AS) is a collection of routers & n/ws under a single administration authority.
- Routing inside an AS is called Intradomain Routing.
- Routing between AS is called Interdomain Routing.

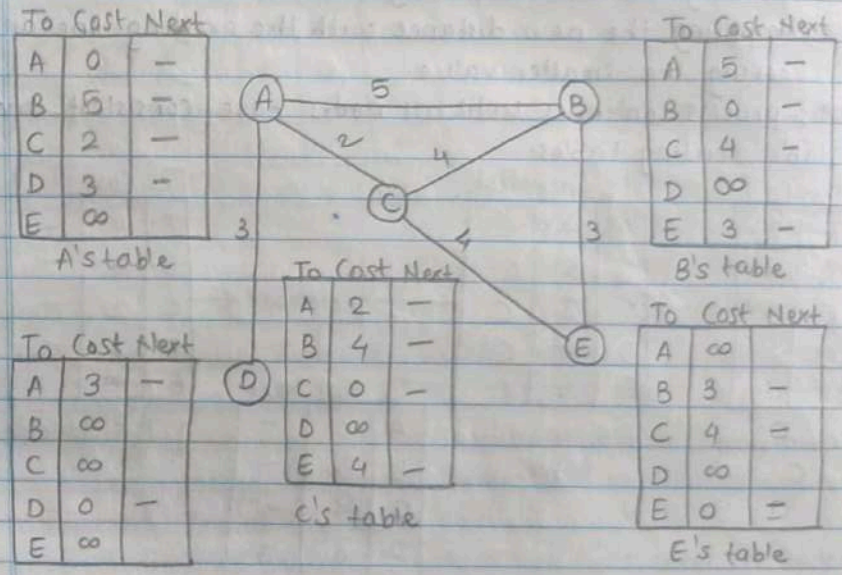


§ Distance Vector Routing (DVR):

- DVR is a dynamic routing protocol in which each node (router) maintains a table, called the distance vector.
- This table contains the minimum distance (cost) to reach every other node in the network and the corresponding next-hop router.
- Principle: The router with the least cost is always selected.
- Each node initially knows only the distance to its direct neighbours. By exchanging information with neighbours, the node gradually learns the shortest path to all other nodes.

- Working:

1. Initialization:
↳ At the beginning, each node knows only the cost to reach its immediate neighbors
↳ The distance to non-neighboring nodes is marked as infinity.



2. Sharing of Tables:
↳ Each node periodically shares its routing table (only destination and cost columns) with its immediate neighbors.

(Prof. Tejal Rane)

↳ Neighbors use this information to update their own routing tables.

↳ The next-hop entry in the table is replaced with the sender's name.

3. **Updating of Tables:**

↳ On receiving a neighbor's table, a node updates its own table by:

→ Adding the cost of the link to the neighbor

→ Updating the next-hop entry.

→ Comparing the new distance with the existing one and keeping the smaller value.

↳ This process continues until all nodes have consistent and stable routing tables.

To	Cost
A	2
B	4
C	0
D	∞
E	4

Received from C

To	Cost	Next
A	4	C
B	6	C
C	2	C
D	∞	C
E	6	C

A's modified table

To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	∞	

A's old table

Compare

To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

A's new table

To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

A's table

To	Cost	Next
A	5	—
B	0	—
C	4	—
D	8	A
E	3	—

B's table

To	Cost	Next
A	3	—
B	8	A
C	5	A
D	0	—
E	9	A

D's table

To	Cost	Next
A	2	—
B	4	—
C	0	—
D	5	A
E	4	—

C's table

To	Cost	Next
A	6	C
B	3	—
C	4	—
D	9	C
E	0	—

E's table

4. **When to Share:**

↳ **Periodic Updates:** Nodes share their tables at fixed intervals (eg. every 30 seconds).

↳ **Triggered Updates:** Whenever a change occurs (eg. link failure), nodes immediately share updates with neighbours.

- **Problems and Instability:**

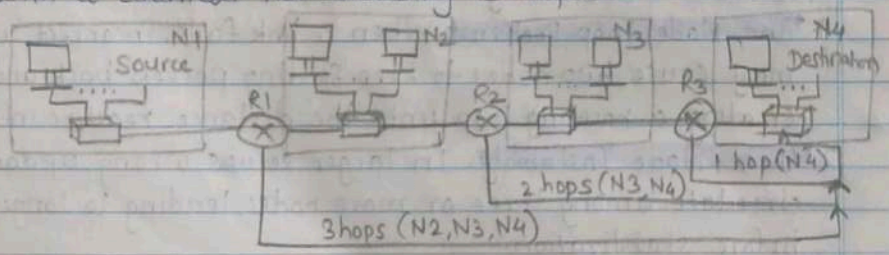
1. **Two-Node Loop Problem:** When a link fails, incorrect updates may cause two nodes to keep sending packets back and forth, creating a routing loop until the distance reaches infinity.
2. **Three-Node Instability:** In larger setups, wrong updates may circulate among three or more nodes, leading to longer loops before stabilization.

(Prof. Tejal Rane)

- Solutions to Instability:
  ↳ **Defining Infinity**: Limit infinity to a small number (eg. 16). This reduces convergence time but restricts n/w size.
  ↳ **Split Horizon**: Prevents a router from advertising a route back to the neighbour from which it learned that route.
  ↳ **Poison Reverse**: A stronger version of split horizon where a router explicitly advertises the route back to the source with an infinite distance to prevent loops.

Routing Information Protocol (RIP):

- RIP is based on distance-vector routing algorithm.
- Hop Count as the Metric:
  ↳ In RIP, the cost of reaching a destination is measured in terms of hop count i.e. the no. of routers a packet must pass through to reach its destination.
  ↳ The source network itself is not counted because the host simply delivers the packet to its default router.
  ↳ The maximum hop count allowed in RIP is 15. A hop count of 16 is considered infinity, which means the destination is unreachable.
  ↳ Due to this limitation, RIP is suitable only for small n/ws with a diameter not exceeding 15 hops.



Hop counts in RIP

- Forwarding Table in RIP:
  ↳ Each router maintains a forwarding table with three fields:
    1. Destination Network Address.
    2. Next-Hop Router
    3. Cost.
  ↳ Ex: If R1 wants to reach Network N4 the table may specify R2 as the next hop. Then R2 specifies R3 as the next hop, and finally R3 delivers to N4.
  ↳ The cost is not directly used for forwarding but is essential for updating the table when route changes occur.

Forwarding table R1

Destination network	Next router	Cost in hops
N1	—	1
N2	—	1
N3	R2	2
N4	R2	3

Forwarding table for R2

Destination n/w	Next router	Cost in hops
N1	R1	2
N2	—	1
N3	—	1
N4	R3	2

Forwarding table for R3

Destination n/w	Next router	Cost in hops
N1	R2	3
N2	R2	2
N3	—	1
N4	—	1

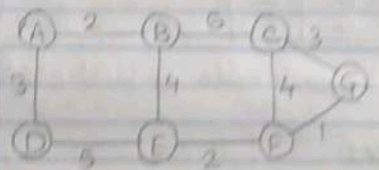
- RIP Messages:
  ↳ RIP messages are encapsulated inside UDP datagrams and transmitted on port 520.
  ↳ RIP defines two message types:
    1. **Request Message**: Sent by a router that has just started or when it wants specific routing information.
    2. **Response (Update) Message**: Can be solicited (in reply to a request) or unsolicited (periodic updates).

(Prof. Tejal Rane)

- **RIP Algorithm**: RIP follows the distance-vector routing algorithm with some modifications:
  - ↳ Instead of sending only distances, a router sends its entire forwarding table in update messages.
  - ↳ On receiving the table from a neighbor, a router:
    1. Adds one hop to each received cost.
    2. Updates the next-hop field to the address of the sending router
    3. Compares new routes with old ones and updates only if:
       - → The new route does not exist in the table
       - → The new cost is lower than the old one
       - → The new cost is higher but learned from the same next-hop router
- **Timers in RIP**: RIP uses three types of timers to maintain efficiency and stability.
  1. **Periodic Timer**: Sends update messages at random intervals between 25-35 seconds to avoid synchronization.
  2. **Expiration Timer**: Each route has an expiration timer (180 seconds). If no update is received within this time, the route is marked invalid with hop count = 16.
  3. **Garbage-Collection Timer**: When a route becomes invalid, it is not immediately deleted. Instead, it is advertised with hop count = 16 for 120 seconds before being purged.
- **Limitations**:
  - ↳ Maximum hop count = 15 makes it unsuitable for large networks.
  - ↳ Convergence is slow compared to modern protocols.
  - ↳ Prone to 'count-to-infinity' problem, though techniques like split horizon and poison reverse are used to reduce this issue.

Link-State Routing (LSR):

- Routing algorithm that creates least-cost trees directly.
- Each router maintains a complete map of the network.
- Uses Link-State Packets (LSPs) and flooding to share information.
- **Link-State Database (LSDB)**
  - ↳ Collection of link-states = Link-State Database
  - ↳ Each node builds the same LSDB it ensures consistency.
  - ↳ LSDB allows each router to run shortest-path calculations.



a. The weighted graph

	A	B	C	D	E	F	G
A	0	2	∞	5	∞	∞	∞
B	2	0	5	∞	4	∞	∞
C	∞	5	0	∞	∞	4	3
D	5	∞	∞	0	5	∞	∞
E	∞	4	∞	5	0	2	∞
F	∞	∞	4	∞	2	0	1
G	∞	∞	3	∞	∞	1	0

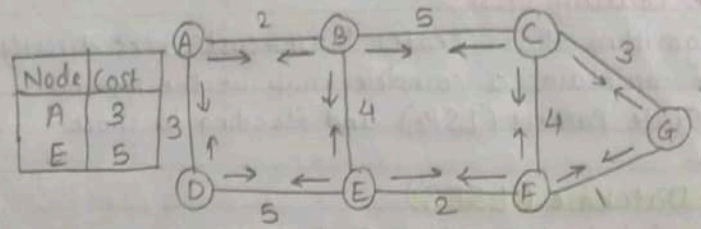
b. Link-state database

- **Link-State Packet (LSP)**:
  - ↳ Contains: 1. Identity of neighbor
    2. Cost of the link
  - ↳ Generated by sending Hello (greeting) messages to neighbors.
  - ↳ Distributed through the network using flooding.
  - ↳ Sequence numbers ensure routers keep only the latest LSP.
- **Flooding Process**
  - ↳ Router forwards received LSPs to all neighbors except the sender.
  - ↳ Old LSPs discarded; only newest retained.
  - ↳ Flooding stops naturally (last node with single interface).

Node	Cost
B	2
D	3

Node	Cost
A	2
C	5
E	4

Node	Cost
B	5
F	4
G	3



Node	Cost
A	3
E	5

Node	Cost
C	3
F	1

Node	Cost
B	4
D	5
E	2

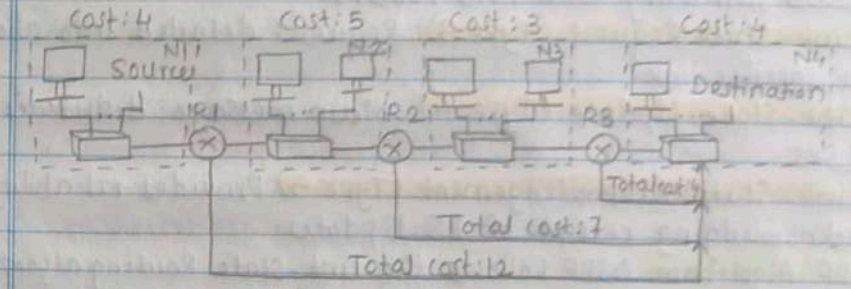
Node	Cost
C	4
E	2
G	1

LSPs created and sent by each node to build LSDB

- **Formation of Least-Cost Trees**
  - ↳ Each router runs Dijkstra's Algorithm on LSDB:
    1. Choose self as root
    2. Select nearest node not in tree then add to tree.
    3. Update costs to other nodes.
    4. Repeat until all nodes are added.
  - ↳ Produces a shortest path tree (SPT) which is used to form forwarding table.
- **Advantages of LSR:**
  - ↳ Provides loop-free and optimal routes
  - ↳ Fast convergence (updates propagate quickly).
  - ↳ Each router has global knowledge of the network.

Open Shortest Path First (OSPF):

- OSPF is an intradomain routing protocol based on link-state routing.
- Unlike RIP (distance vector, hop count), OSPF uses link cost/metric that can be assigned based on bandwidth, delay, reliability or throughput.
- Provides faster convergence and supports large networks
- **Metric:**
  - ↳ Each link is assigned a cost (weight) according to performance parameters.
  - ↳ The total cost of a path is the sum of the costs of its links.
  - ↳ Routers use Dijkstra's Algorithm to compute the shortest path tree (SPT).
  - ↳ The result of SPT is stored in the forwarding table of each router.



Metric in OSPF

- **Areas:**
  - ↳ In small AS: LSP flooding is manageable
  - ↳ In large AS: flooding everywhere causes excessive traffic.
  - ↳ Solution: Divide AS into areas.
    - → Each area maintains its own LSDB.
    - → A special Backbone Area connects all other areas.
    - → Routers in the backbone distribute routing information between areas.
  - ↳ This design makes OSPF scalable for large networks.

Forwarding table for R1

Dest N/w	Next router	Cost
N1	—	4
N2	—	5
N3	R2	8
N4	R2	12

Forwarding table for R2

Dest N/w	Next router	Cost
N1	R1	9
N2	—	5
N3	—	3
N4	R3	7

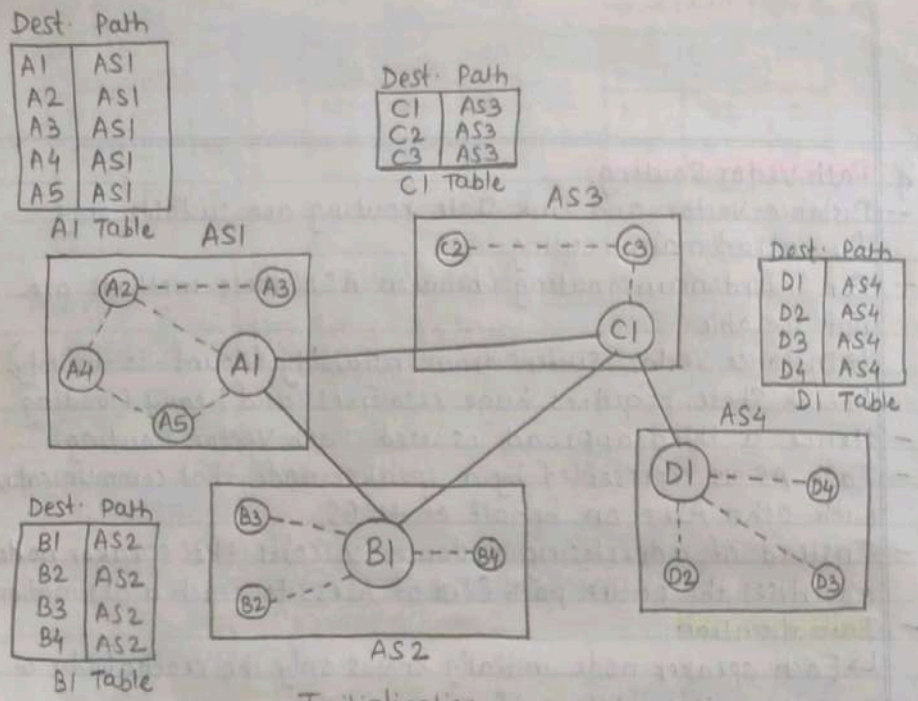
Forwarding table for R3

Dest N/w	Next Router	cost
N1	R2	12
N2	R2	8
N3	—	3
N4	—	4

- OSPF messages are carried in IP datagrams with protocol field = 89.
- Two main versions exist: OSPFv1 and OSPFv2
- **OSPF Messages (5 Types):**
  1. **Hello Message (Type 1):** Introduces a router to its neighbours.
  2. **Database Description (Type 2):** Sent after Hello to share LSDB summary with new routers.
  3. **Link-State Request (Type 3):** Requests detailed info about a specific link.
  4. **Link-State Update (Type 4):** Main message; distributes LSPs.
  5. **Link-State Acknowledgement (Type 5):** Provides reliability by acknowledging receipt of LS Updates.
- **OSPF Algorithm:** OSPF follows the Link-State Routing algorithm:
  (1) Collect LS information via LSP flooding.
  (2) Build LSDB for the area.
  (3) Run Dijkstra's Algorithm to form the SPT.
  (4) Create forwarding table.
- **Advantages:**
  ↳ Supports large and hierarchical networks (via areas).
  ↳ Provides fast convergence and loop-free routes.
  ↳ More accurate than RIP (since cost depends on link performance, not just hop count.)

8 Path Vector Routing:

- Distance Vector and Link State routing are suitable only for intradomain routing.
- For interdomain routing (between AS), these methods are not scalable.
  ↳ Distance Vector: Suffers from instability (count-to-infinity)
  ↳ Link State: requires huge resources and heavy flooding.
- Hence a third approach is used: Path Vector Routing.
- Each AS is represented by a speaker node that communicates with other ASes on behalf of its AS.
- Instead of advertising distances or costs, the speaker node advertises the entire path (list of ASes) to reach a destination.
- **Initialization:**
  ↳ Each speaker node initially knows only the reachability of nodes inside its own AS.
  ↳ Example: In a system with AS1, AS2, AS3, AS4.
    → Speaker A1 in AS1 advertises that all A nodes are in AS1.
    → Speaker B1 in AS2 advertises B nodes, and so on.
- **Sharing:**
  ↳ Similar to Distance Vector, each speaker shares its routing table with immediate neighbors.
  ↳ Ex: A1 shares with B1 and C1; C1 shares with D1, B1, A1 etc.
  ↳ Gradually, routing tables expand to include nodes in all ASes.
- **Updating:**
  ↳ When a speaker receives a routing table from a neighbor it
    → Adds any new destinations not already in its table.
    → Prepends its own AS number to the path.
  ↳ Over time, each speaker knows the full path to reach any destination node.
  ↳ Ex: If node A1 wants to reach D1, the path may be AS1 → AS2 → AS3 → AS4



Dest.	Path
A1	AS1
...	
A5	AS1
B1	AS1-AS2
...	
B4	AS1-AS2
C1	AS1-AS3
...	
C3	AS1-AS3
D1	AS1-AS3-AS4
...	
D4	AS1-AS3-AS4

A1 Table

Dest.	Path
A1	AS3-AS1
...	
A5	AS3-AS1
B1	AS3-AS2
...	
B4	AS3-AS2
C1	AS3
...	
C3	AS3
D1	AS3-AS4
...	
D4	AS3-AS4

B1 Table

Dest.	Path
A1	AS3-AS1
...	
A5	AS3-AS1
B1	AS3-AS2
...	
B4	AS3-AS2
C1	AS3
...	
C3	AS3
D1	AS3-AS4
...	
D4	AS3-AS4

C1 Table

Dest.	Path
A1	AS4-AS3-AS1
...	
A5	AS4-AS3-AS1
B1	AS4-AS3-AS2
...	
B4	AS4-AS3-AS2
C1	AS4-AS3
...	
C3	AS4-AS3
D1	AS4
...	
D4	AS4

D1 Table

Updation

- Features:
  - ↳ Loop Prevention:
    - → When a router receives an advertised path, it checks if its own AS number already appears in the path.
    - → If yes, the route is discarded (loop avoided)
  - ↳ Policy Routing:
    - → Since full paths are known, an AS can apply policies (eg., ignore routes passing through certain ASes)
    - → Useful for security, trust or business policies.
  - ↳ Optimum Path:
    - → No single metric (like RIP hop count or OSPF delay) is used.
    - → The best path depends on organizational choice - eg., shortest AS path, most reliable, secure, or policy-based.

- Advantages:
  - ↳ Scalable for large interdomain networks
  - ↳ Prevents loops efficiently
  - ↳ Supports flexible policy-based routing.

§ Border Gateway Protocol (BGP):

- BGP is the interdomain routing protocol of the internet.
- It is based on Path Vector Routing, where each update carries the complete path (list of ASes) to reach a destination.
- BGP has evolved through four versions, the current widely used version is BGP-4.
- Types of Autonomous System (AS): Depending on connectivity ASes are classified as:
  - (1) Stub AS:
    - ↳ Connected to only one other AS.
    - ↳ Acts only as a source or sink of traffic (no transit traffic)
    - ↳ Ex: A small ISP or small corporate network.
  - (2) Multihomed AS:
    - ↳ Connected to multiple ASes.
    - ↳ Still acts only as a source or sink, i.e., no transit allowed.
    - ↳ Ex: A large corporation connected to multiple ISPs.

(3) Transit AS:
↳ Connected to multiple ASes and allows transit traffic.
↳ Ex: Large national or international ISPs

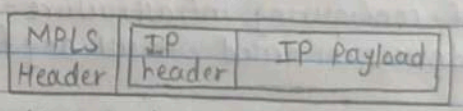
- Path Attributes in BGP:
↳ In BGP, a path is not just a list of ASes, but a list of attributes.
↳ Attributes help routers make policy-based routing decisions.
↳ Attributes are classified as:
(1) Well-known Attributes:
→ Must be recognized by every BGP router.
→ Divided into:
• Mandatory (must appear in every update):
∘ ORIGIN → Source of routing info (RIP, OSPF, etc.)
∘ AS_PATH → List of ASes along the path.
∘ NEXT_HOP → The next router to forward the packet.
• Discretionary (recognized, but not required in every update).
(2) Optional Attributes:
→ May or may not be implemented in all routers.
→ Divided into:
• Transitive (must be forwarded even if not understood).
• Non-Transitive (discarded if not recognized).

- BGP Sessions:
↳ Routing information in BGP is exchanged using sessions between routers.
↳ A session is a semi-permanent TCP connection (port 179) between two BGP routers.
↳ The connection is reliable since it uses TCP, and it can last for a long time.
↳ This ensures stable and policy-controlled routing updates.

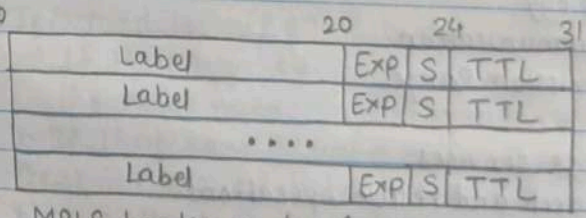
- External vs Internal BGP:
↳ External BGP (E-BGP):
→ Session between two routers belonging to different ASes.
→ Used for exchanging interdomain routes.
↳ Internal BGP (I-BGP):
→ Session between routers inside the same AS.
→ Used to distribute routes learned from E-BGP to other routers within the AS.

8) Multiprotocol Label Switching (MPLS):
- MPLS is high-performance forwarding technology approved by the IETF. It combines the advantages of routing and switching. MPLS routers can forward packets either:
↳ Based on the destination IP address, or
↳ Based on a short label attached to the packet.
This makes MPLS faster, flexible, and suitable for supporting multiple protocols.

- MPLS Header:
Since IPv4 packets cannot be directly extended with labels, MPLS encapsulates the entire IP packet inside an MPLS packet, placing an MPLS header between the DLL and network layer.
↳ The MPLS header is a 32-bit (4-byte) sub-header.
↳ Multiple such headers can be stacked together for hierarchical switching.



MPLS Header added to an IP packet



MPLS header made of a stack of labels.

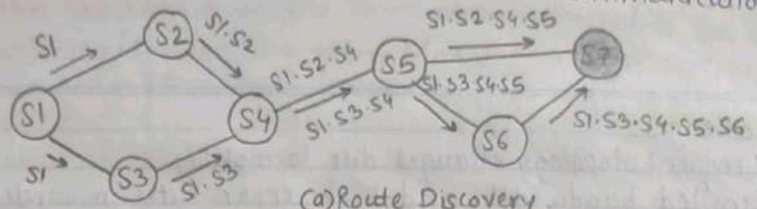
- MPLS Header fields:
(1) Label (20 bits): A unique short identifier used to the index the switching/forwarding table. Makes packet forwarding faster than long IP address lookup.
(2) Exp (3 bits): Reserved for experimental use (QoS priority, etc).
(3) S (1 bit): Stack field. If S=1, it means this is the last label in the stack.
(4) TTL (8 bits): Similar to IP TTL. Decremented at every hop to prevent routing loops.
- Hierarchical Switching: MPLS supports stacked headers, which allows multi-level or hierarchical switching:
↳ The top label is used to forward the packet in a larger network.
↳ The bottom label is used inside an organization to route to a specific subnet or final host.
This makes MPLS scalable and efficient, supporting both large-scale backbone routing and local subnet forwarding.
- Advantages:
(1) Faster packet forwarding (uses labels instead of long IP lookup).
(2) Supports multiple protocols (IPv4, IPv6, ATM, Frame Relay).
(3) Efficient for VPNs, traffic engineering and Quality of service (QoS).
(4) Provides flexibility of routing with the efficiency of switching.

§ Mobile Ad-Hoc Network (MANET):
- A MANET is a self-configuring, infrastructure-less wireless network of mobile devices connected without any fixed base stations.
- Key features:
(1) Infrastructure-less
(2) Dynamic Topology
(3) Multi-hop communication.
(4) Limited Transmission Range
- Applications:
(1) Military/defense services.
(2) Emergency search and rescue operations
(3) Disaster recovery.
(4) Conferences, meetings, and temporary setups where quick info exchange is needed.

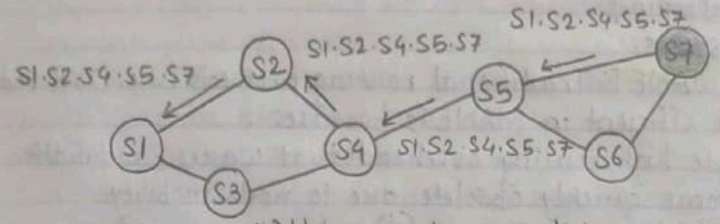
- Challenges:
(1) Frequent topology changes due to mobility.
(2) Limited bandwidth and high error rates in wireless links.
(3) Energy constraints.
(4) Security issues.
- Routing in MANET: Traditional routing protocols like DVR and LSR are not efficient in MANETs because:
(1) They create high routing overhead that wastes bandwidth.
(2) Routes become quickly obsolete due to node mobility.
Hence, specialized MANET routing protocols are used.

§ Dynamic Source Routing (DSR) Protocol
- DSR is a reactive (on-demand) routing protocol designed for Mobile Ad Hoc Networks (MANETs). A route is discovered only when required, reducing unnecessary routing overhead.
- Phases of DSR: DSR works in two main phases:
(1) Route Discovery:
↳ When a source node wants to send data, it first checks its route cache for an existing route.
↳ If no route exists, it broadcasts a Route Request (RREQ) to its neighbors.
↳ The RREQ contains: Source address, Destination address, Unique request ID.
↳ Intermediate nodes:
→ If they have no route, they add their address to the route record and rebroadcast.
→ If they have a valid route, they may reply directly.
↳ Once the request reaches the destination node, it sends back a Route Reply (RREP) containing the discovered path.

↳ The source caches this route for future communication.



(a) Route Discovery.



(b) Using route record to send the route reply

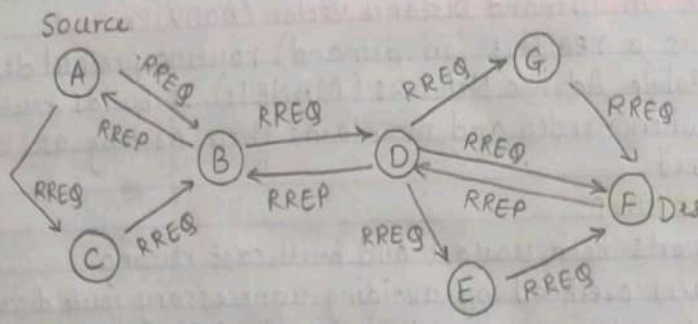
(2) Route Maintenance:
- ↳ Since MANET topologies change frequently, routes may break.
- ↳ Each node confirms the reachability of its next hop.
- ↳ If no acknowledgment is received after several retransmissions, the link is considered broken.
- ↳ A Route Error (RERR) message is sent back to the source to trigger a new discovery if needed.

- Advantages:
  (1) Reduces overhead (routes maintained only for active connections).
  (2) Route cache speeds up route discovery.
  (3) One discovery may generate multiple routes via intermediate replies.
- Disadvantages:
  (1) Packet header size increases with route length (source routing)
  (2) Flooding of RREQs may cause network congestion.
  (3) Collisions possible due to multiple broadcasts.
  (4) Stale caches may mislead routing decisions.
- Applications: Works well in MANETs with up to ~200 nodes and can also integrate with cellular/mobile networks.

8) Ad-hoc On Demand Distance Vector (AODV) Protocol:
- AODV is a reactive (on-demand) routing protocol designed for Mobile Ad-hoc Networks (MANETs). It builds routes only when needed and maintains them as long as required.
- Key features:
  (1) Supports both unicast and multicast routing.
  (2) Reduces overhead by avoiding unnecessary route discovery.
  (3) Stores routes in routing tables, unlike DSR
- Phases of Operation:
  (1) Route Discovery:
    (i) Initiated when a source node wants to send data and has no route.
    (ii) The source broadcasts a Route Request (RREQ).
    (iii) Intermediate nodes forward the RREQ and record the previous hop (creating temporary reverse paths).
    (iv) When the RREQ reaches the destination, a Route Reply (RREP) is sent back along the reverse path.
    (v) The source then chooses the shortest hop count path.
  (2) Route Maintenance:
    (i) If a link fails, a Route Error (RERR) message is sent to the source.
    (ii) The source can then reinitiate route discovery if communication is still needed.
- Advantages:
  (1) On-demand route discovery reduces unnecessary overhead.
  (2) Routing tables reduce packet header size compared to DSR.
  (3) Supports large and dynamic networks.
  (4) Supports both unicast and multicast communication.
- Disadvantages:
  (1) Initial route discovery causes high latency.

↳ The source caches this route for f.u..

(2) Frequent RREQ floods may cause congestion in large networks.
(3) Broken links require rediscovery, adding delay.
(4) Route maintenance overhead increases with node mobility.



§ Mobile IP:
- Mobile IP is a protocol that enables a host or node to move across different networks while maintaining the same permanent IP address. This ensures continous computing activities without interruption when the host changes its point of attachment.
- Important Entities:
(1) Home Agent (HA): Intercepts packets sent to the mobile node's home address and tunnels them to foreign agents.
(2) Foreign Agent (FA): Forwards packets from HA to the mobile host and sends the host's packets to remote hosts.
- Phases of Mobile IP Operation:
(1) Agent Discovery:
• The mobile node discovers available agents (HA and FA).
• Learns its care-of address in the foreign network.
(2) Registration:
• The mobile node registers its care-of address with both HA and FA.
• Ensures that HA knows the current location of the mobile node.

3. Data transfer.
↳ When a remote host sends data:
→ The packet is first sent to the mobile host's home address.
→ The home agent intercepts and encapsulates it (tunneling).
→ The encapsulated packet is sent to the foreign agent.
→ The foreign agent decapsulates and delivers the packet to the mobile host.
↳ When the mobile host sends data:
→ It uses its home address as the source, and sends the packet through the foreign agent directly to the remote host.
→ No tunneling is required in this case.
- Advantages:
(i) Provides seamless mobility across networks.
(ii) Maintains ongoing sessions without interruption.
(iii) Transparent to users and applications.
- Disadvantages:
(i) Tunneling increases overhead.
(ii) May lead to triangular routing.
(iii) Security concerns due to encapsulation and redirection.