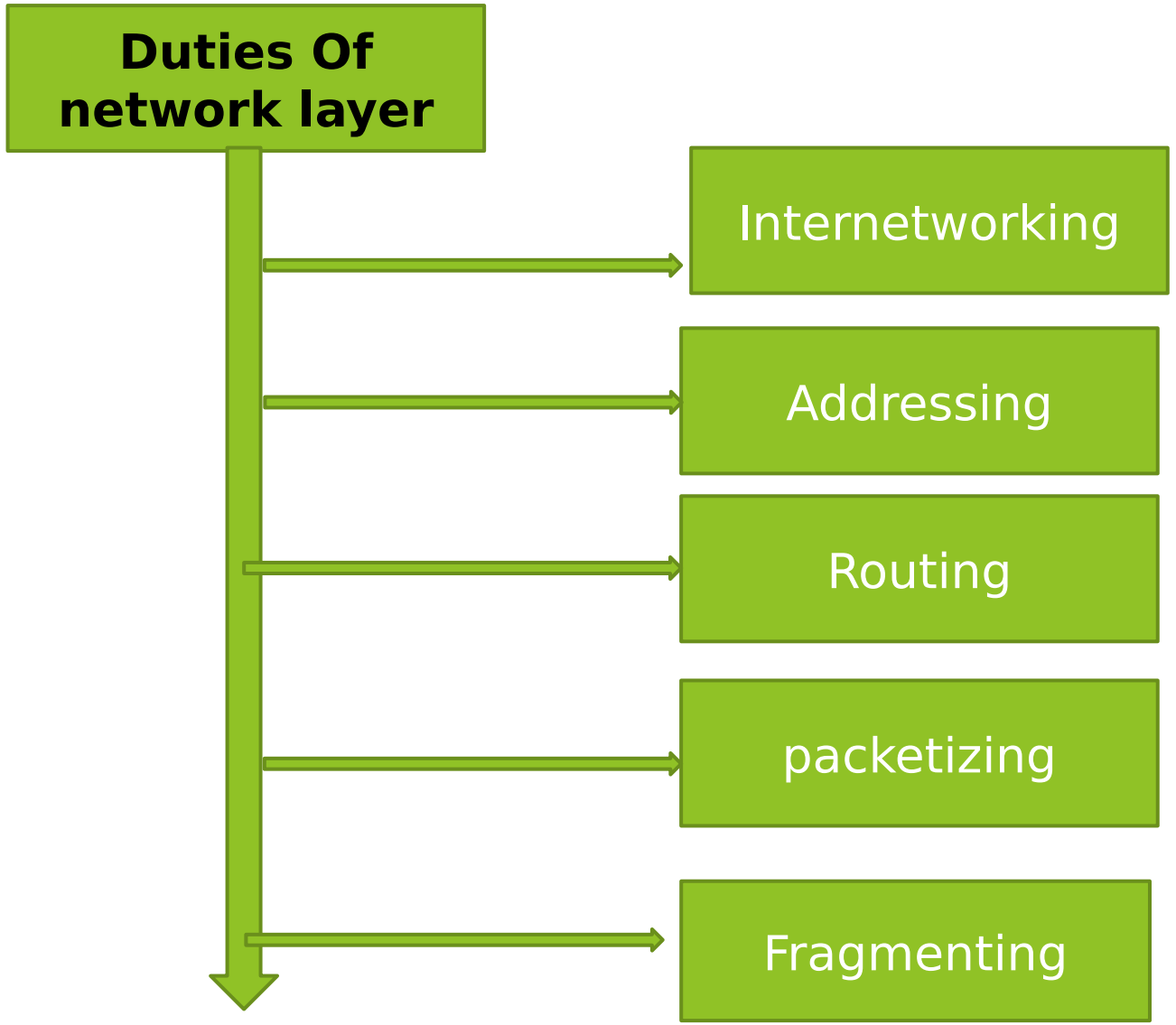
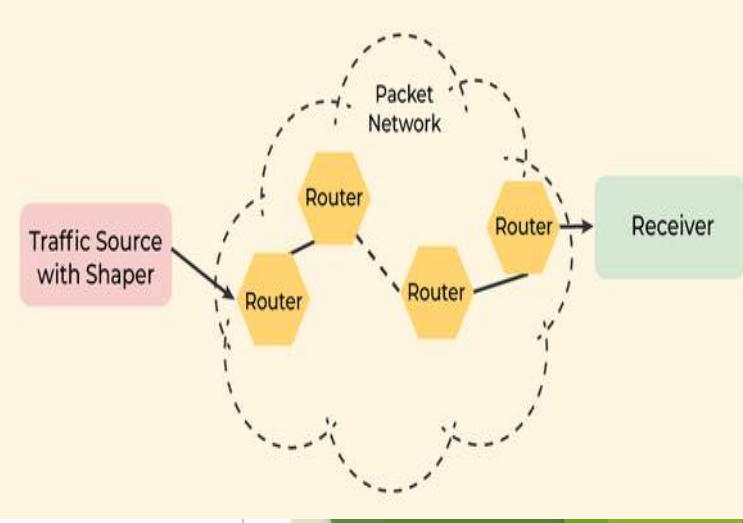
Unit III
Network Layer

Introduction

- The network layer is responsible for **carrying the packet from source to destination.**
- Its main job is to **move data packets between different networks.**
- It helps **route these packets from the sender to the receiver** across multiple paths and networks.
- In the 7-layer OSI model, **the network layer is layer 3**. The **Internet Protocol (IP) is a key protocol** used at this layer

Introduction



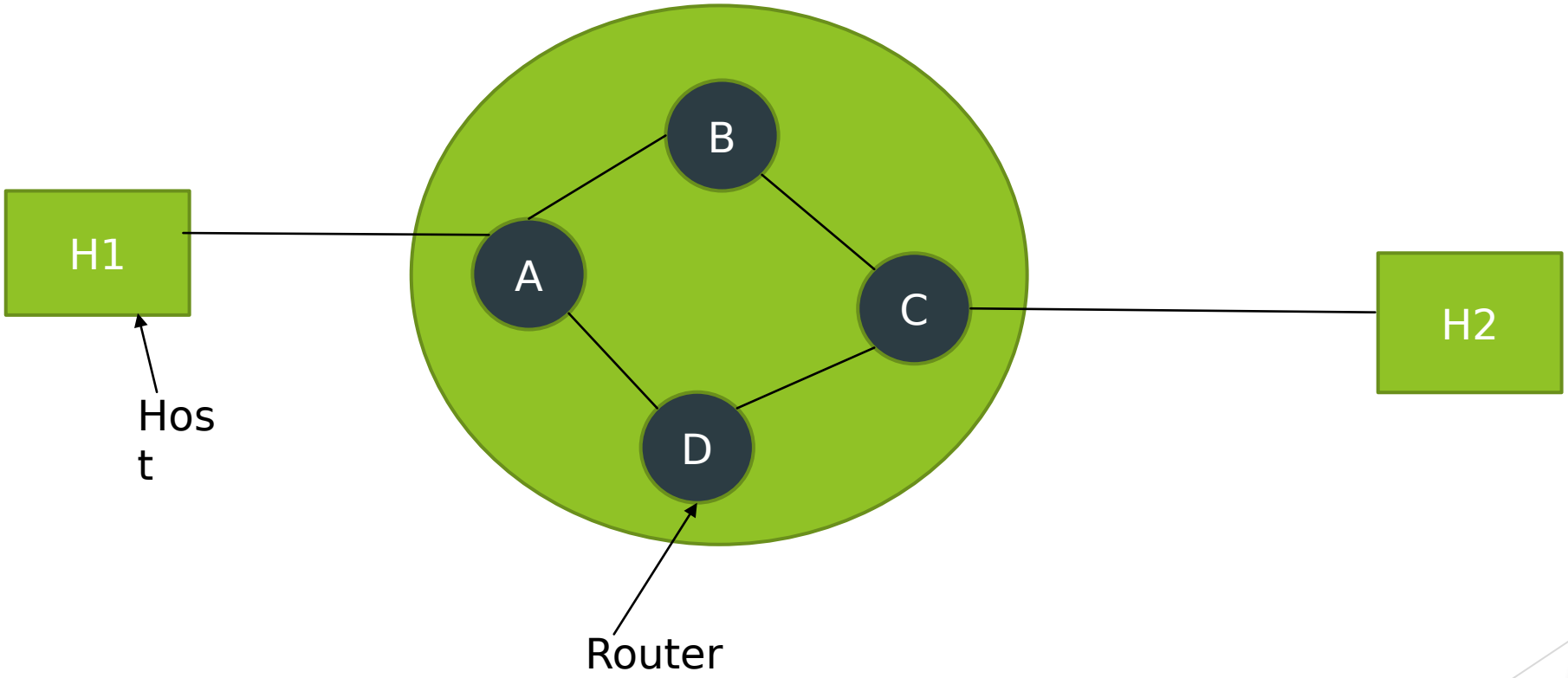


- Internetworking: provides **logical connection** between different types of network.
- Addressing: addressing is necessary to **find out the device** on networking .
- Routing: multiple roots available from source to destination.**network layer is helpful to determine which to be chosen.**
- Packetizing: n/w layer receive packet from upper layer &encapsulate them to form new packet.
- Fragmenting: datagram travel throw different n/w. router de capsulate the IP datagram from received frames.

Network layer design issue (question Ask)

- Store & forward packet switching
- Services provided to transport layer
- Implementation of connectionless service
- Implementation of connection –oriented service
- Internal organization of the network

1)Store & forward packet switching

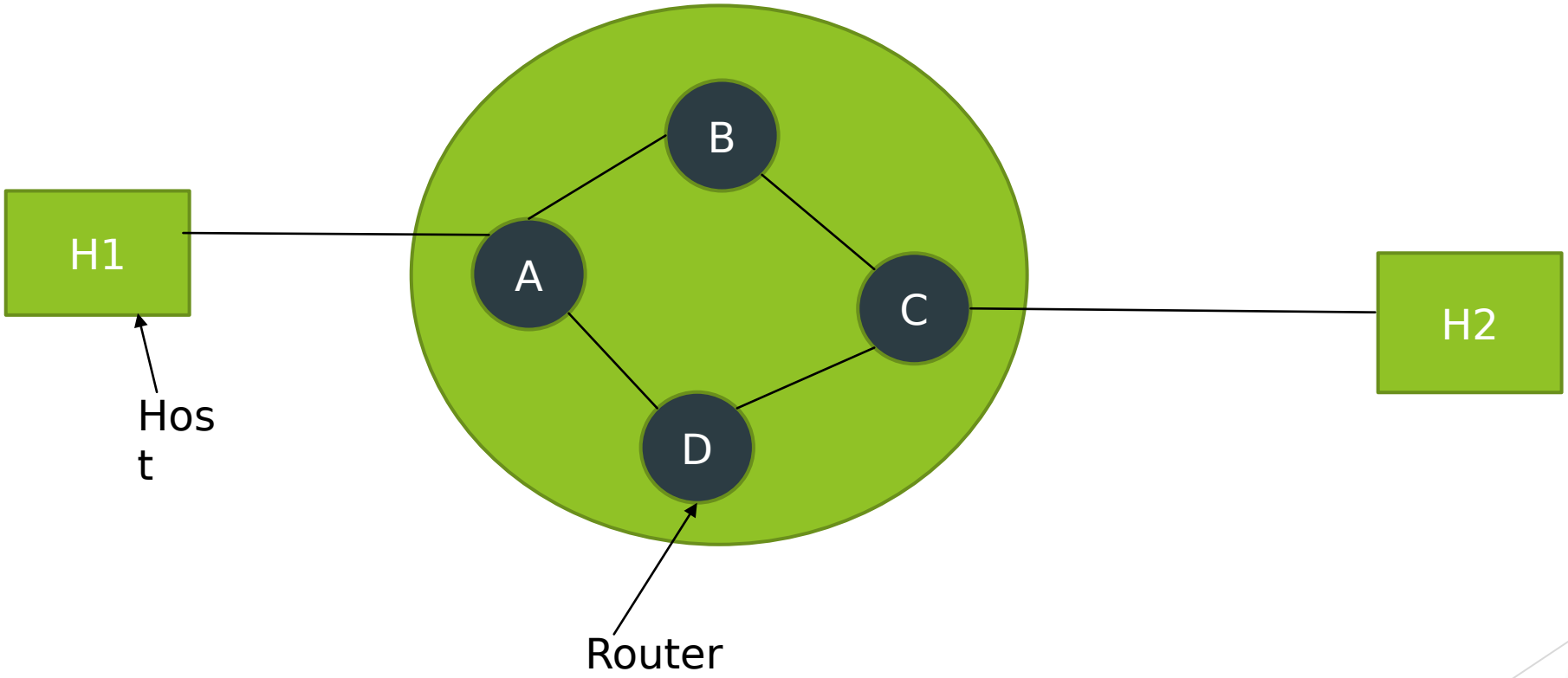


2)Services provided to transport layer

- The services are carefully design with following goals
- 1)Provide services to transport layer **that should be independent of router.**
- **2)network address made available to transport layer** should be uniform.

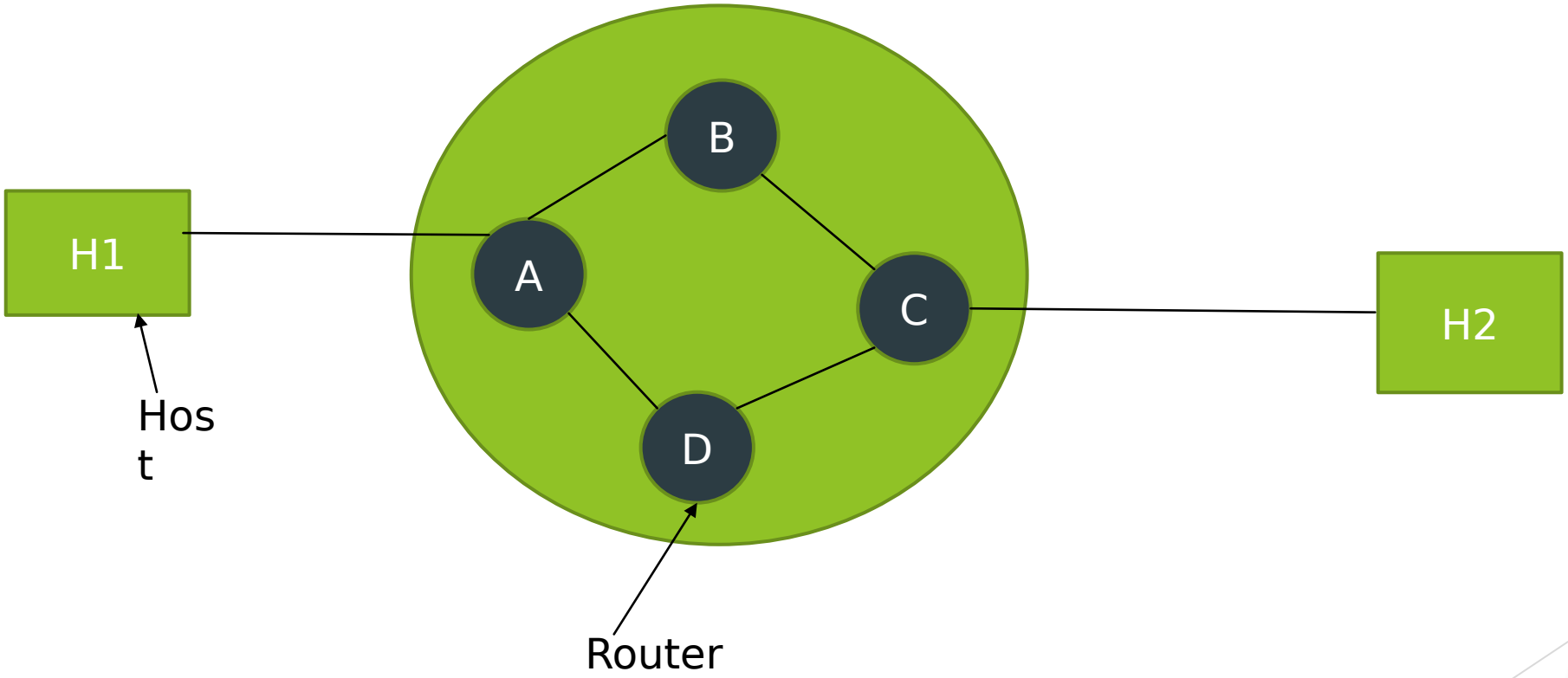
3)Implementation of connection oriented service

(packet consist of virtual circuit number & router consist of routing table)



Implementation of connectionless service

(packet (datagram) consist of destination address.& router don’t hold information about connection)



Internal organization of the network

1)virtual circuits

- Choose **only one** route from source to destination.

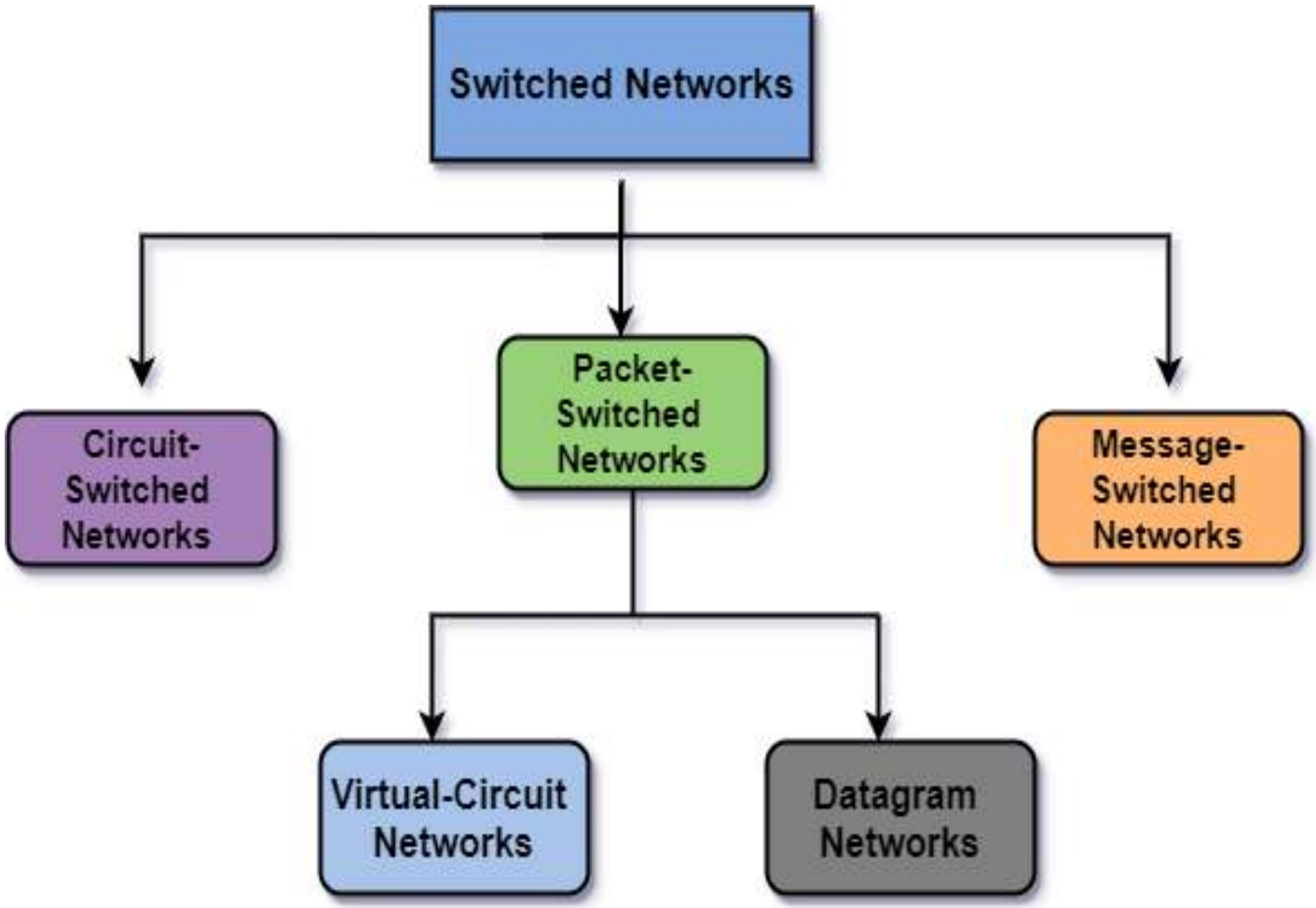
2)datagram

- With datagram routes from source to destination not defined in advanced.
- **Packet can follow the different paths.**

Other services

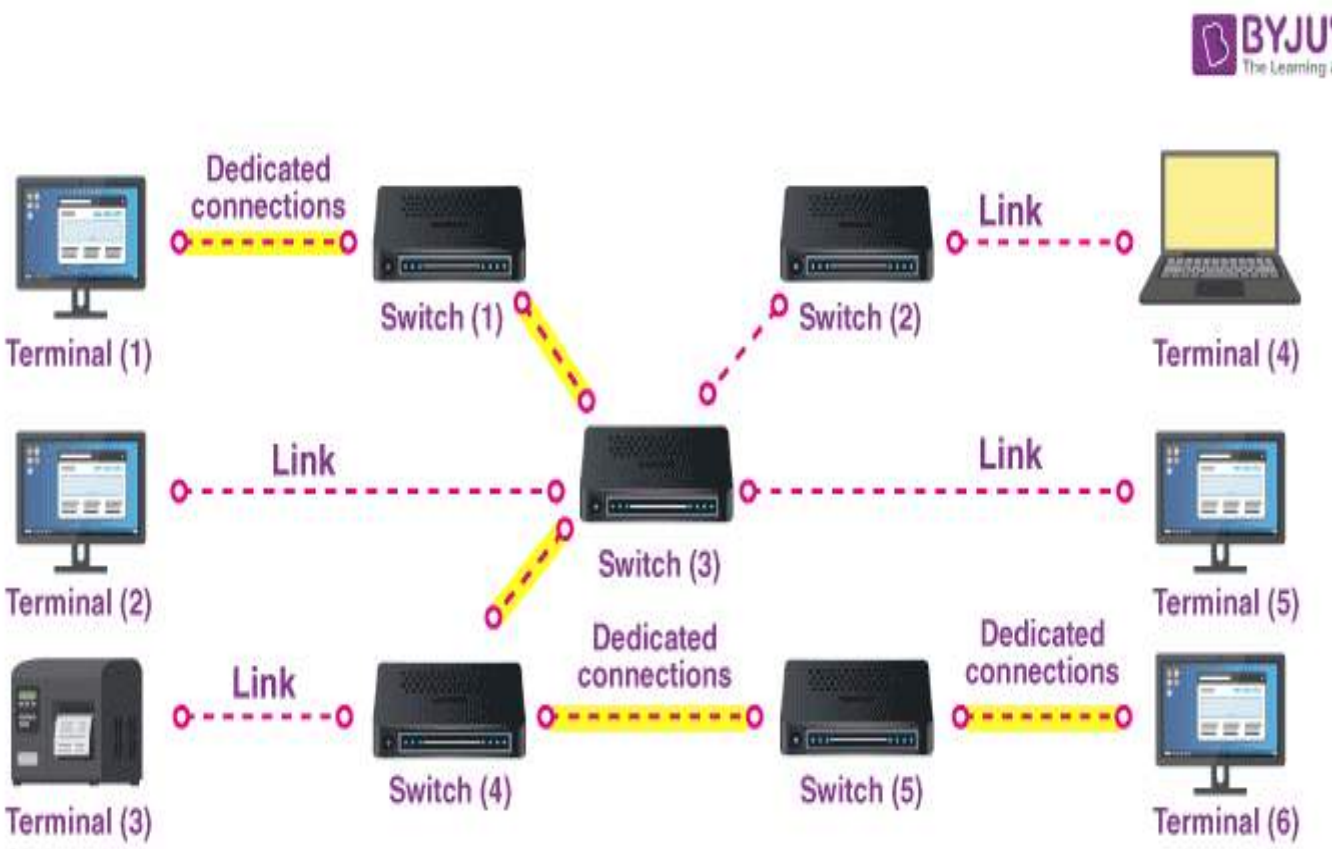
- 1)error control
- 2)flow control
- 3)congestion control
- 4)quality of services
- 5)security

Switching techniques



1)Circuit switching

- **A dedicated path is established between the sender and receiver**.
- **Before data transfer** ,connection will be established first
- Example. Telephone network.
- 3 phases in circuit switching
- 1)connection establishment
- 2)data transfer
- 3)connection disconnection

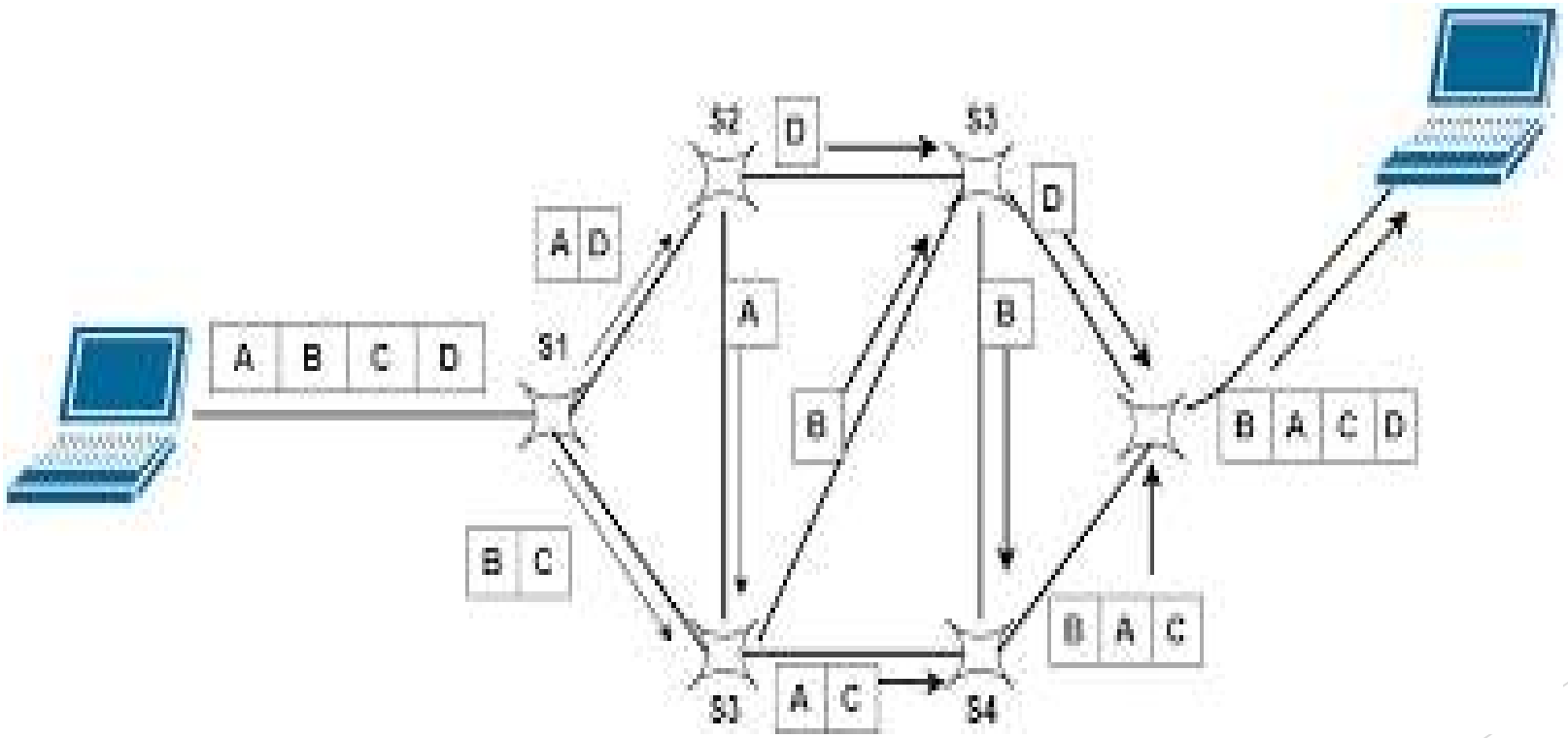

BYJU'S
The Learning App
Dedicated connections
Terminal (1)
Switch (1)
Switch (2)
Link
Terminal (4)
Link
Terminal (2)
Switch (3)
Link
Terminal (5)
Terminal (3)
Link
Switch (4)
Dedicated connections
Switch (5)
Dedicated connections
Terminal (6)

2)Message switching

- Store and forward mechanism
- Message is transferred as a complete unit and forwarded **using store and forward mechanism** of the intermediately node
- Not suited for real time applications.

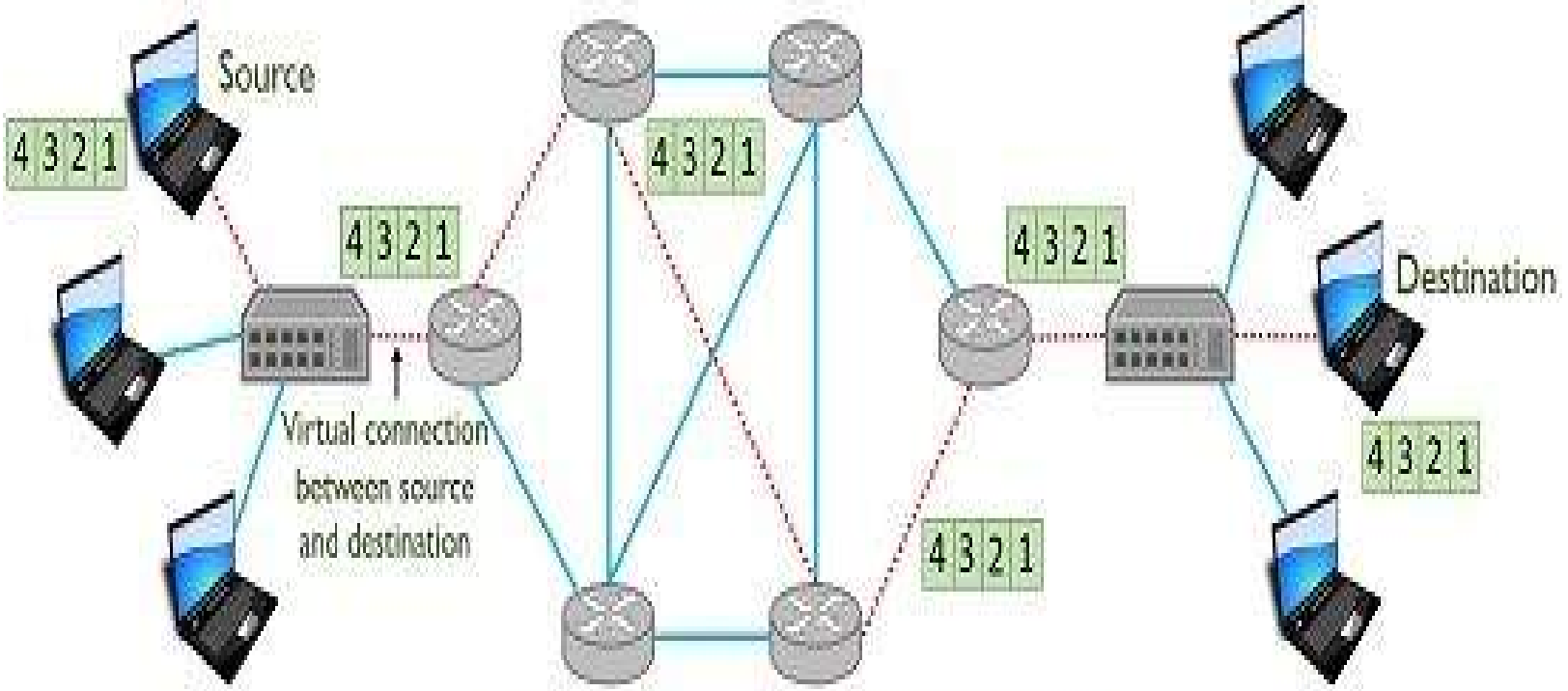
3)Packet switching (datagram)

- The internet is a packet switched network
- Message is broken into chunks called as packet.
- Each packet is sent individually
- Packet consist of source and destination IP address and sequence number
- Sequence number will help the receiver to
- Reorder the packets
- Detect missing packet
- Send ack.


A B C D
S1
S2
S3
S4
A D
D
D
A
B
B
B C
A C
B A C
B A C D

3)Packet switching (virtual circuit)

- virtual circuit switching is also known as connection oriented switching
- In the VC a **preplanned route is established before the message are sent**
- Call request & call accept packets are used to established the connection between sender and receiver.
- **The path is fixed.**



Virtual Circuit Packet Switching

Circuit Globe

Congestion control

- Congestion in a network may occur when the load on the network i.e the **number of packets sent to the network is greater than the capacity of the network.**
- As the **traffic on network increase .they begins loosing of packets.**
- At **very high traffic .performance is completely collapse**.

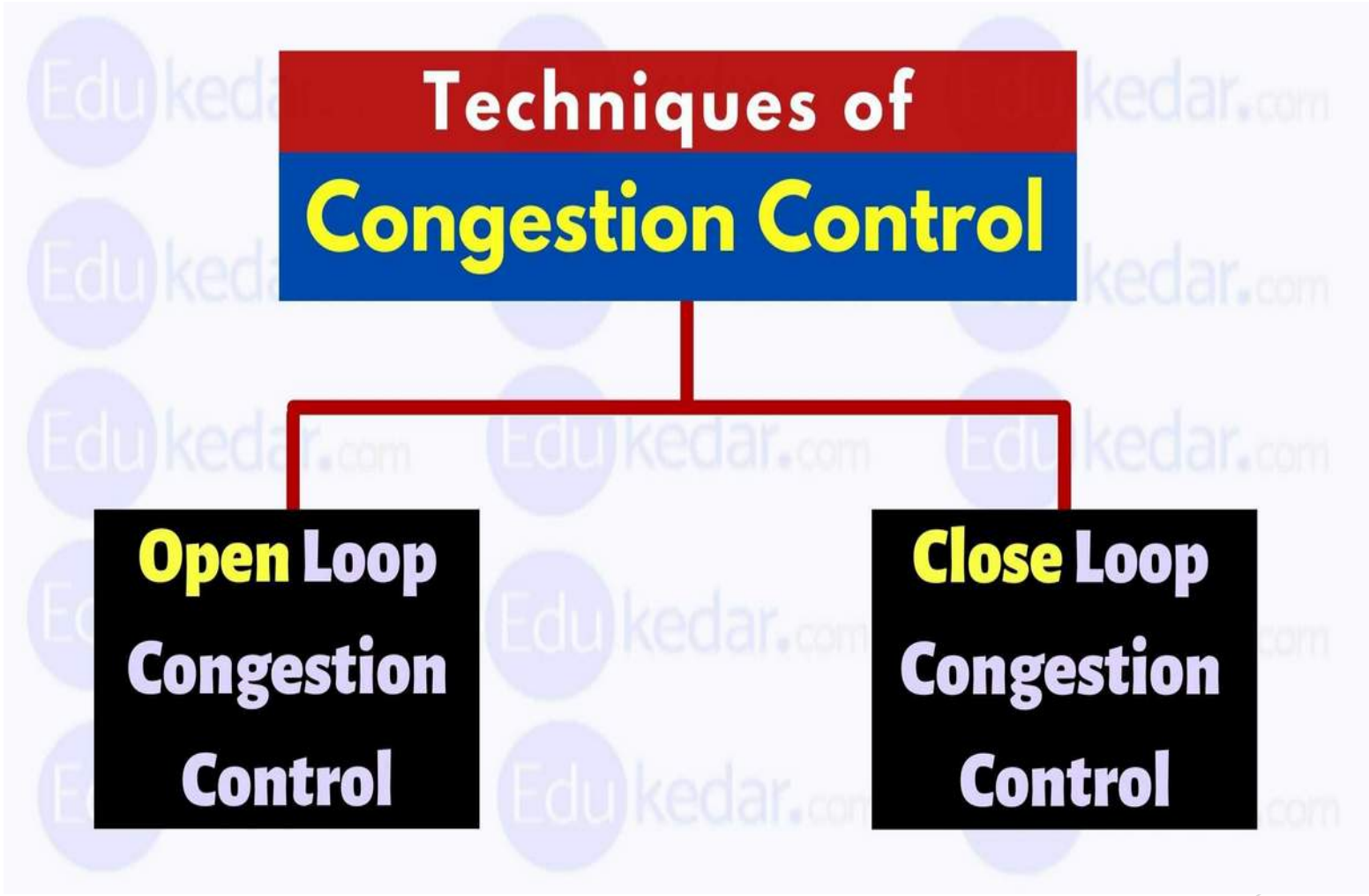
Need of Congestion control

- **For avoiding packet loss we need to control the congestion.**

Causes of congestion

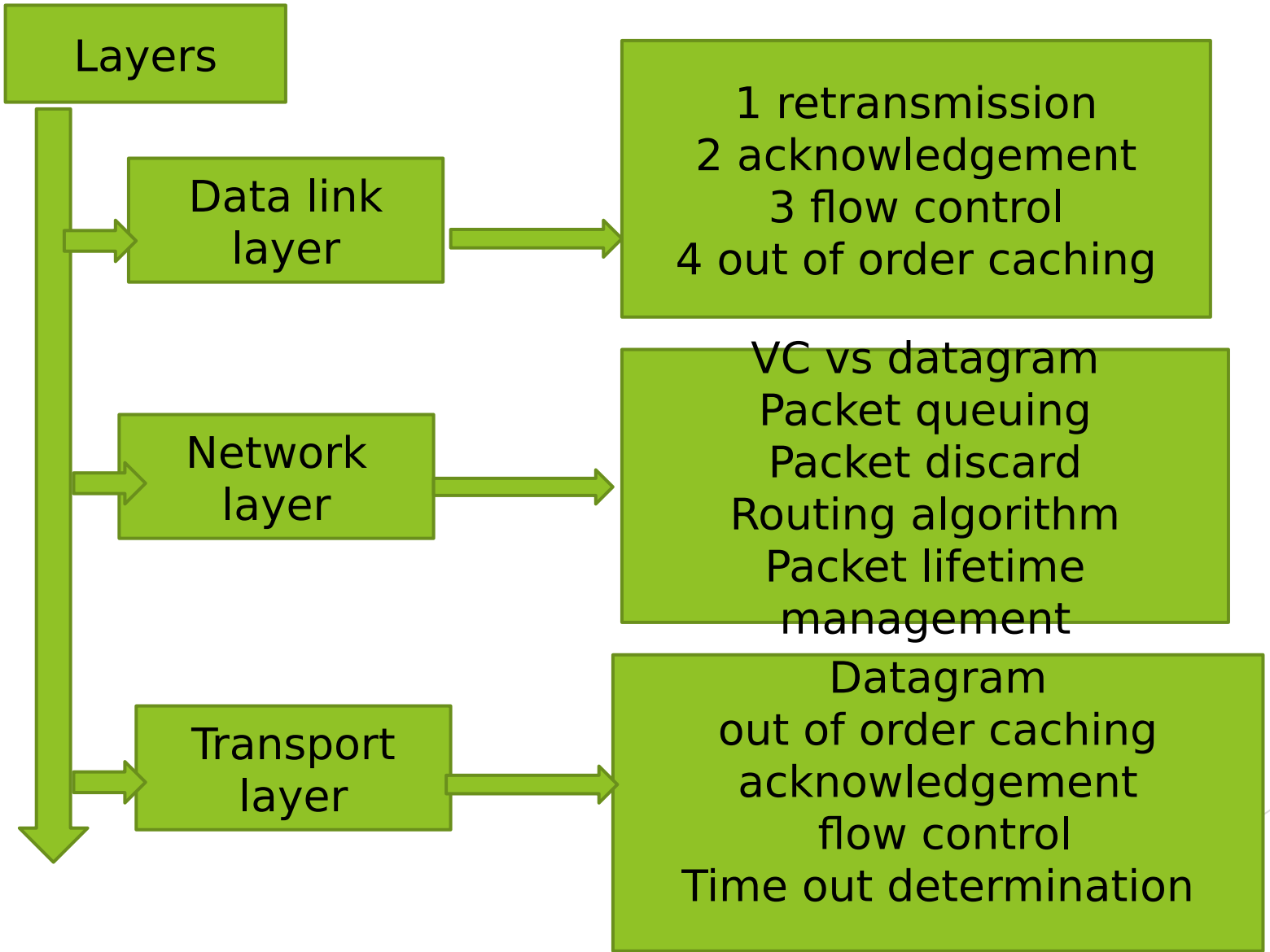
- **1)sudden increase in flow of packets**
- If packets come from 2 or 3 sender & they need same output line.
- Then these packets are queued if memory is not sufficient. Some of packet getting lost.
- **2)presence of slow and low bandwidth**
- Congestion is caused with the slow bandwidth. This problem is solved when we used high speed bandwidth
- **3)use of slow processor**
- Congestion is caused by slow processor. This problem is solved when we improve the speed of processor. faster processor transmit more data.

Principals of congestion control



- **1)open loop control**
- **It prevent the congestion** from happening
- It decide **when to accept packet.& when to discard** the packet.
- **2)closed loop control**
- **It provide the solution after the congestion occur.**
- **Detect** the congestion
- Transfer the **information about congestion**
- **Correct** the congestion

Congestion prevention policy



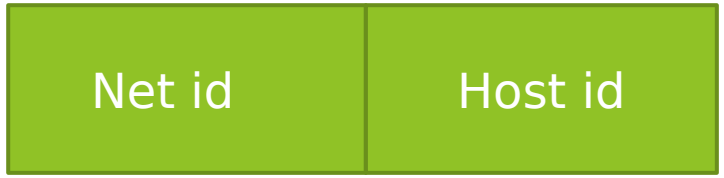
Internet protocol(IP)

- It is a n/w layer protocol used for host to host delivery of packet.
- It is used with TCP/IP protocol
- It carries packet from source to destination in a multiple paths.
- So some packets are miss and loss
- It is when unreliable then paired with UDP.
- Consist of two versions:
- IPv4
- IPv6

IPv4	IPv6
Length 32 bits	Length 128 bit
4 octet addressing	8 octet Addressing
0-255	0-65535
192.168.10.26	3F55.1806.5678.L8ff.3F55.1806.5678.L8ff

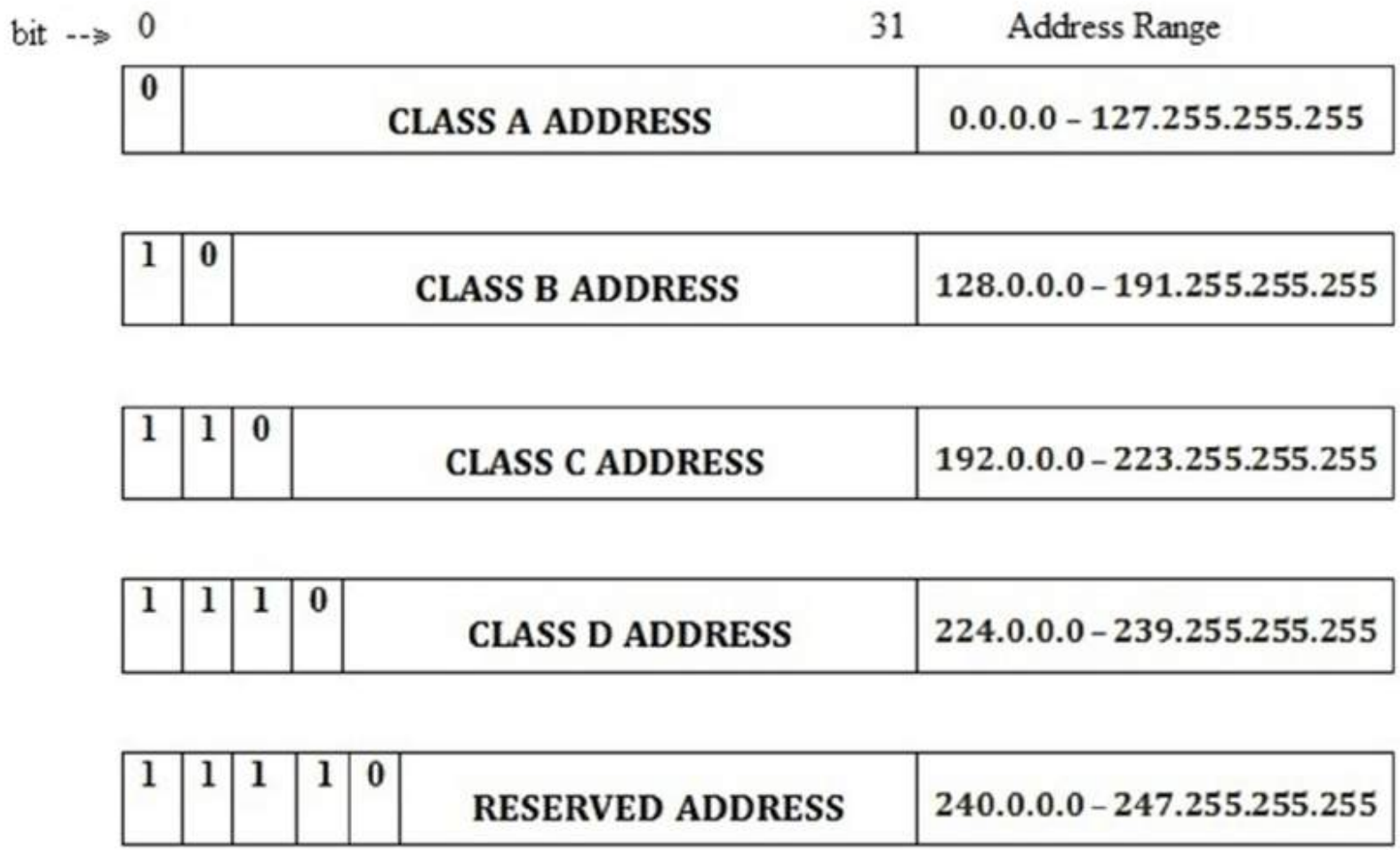
IPv4 address format

- 32 bit
- Net id: identify network on internet
- Host id :identify host on network



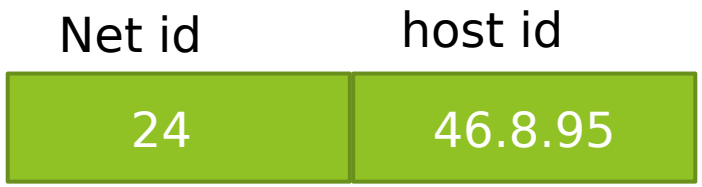
- Consist of five classes:
- Class A
- Class B
- Class C
- Class D
- Class E

- It consist of binary notation and dotted decimal notation
- Binary notation:01110101 10010101 00011101 00000010
- Dotted decimal notation:117.149.29.2
- Notation of IPv4:A,B,C,D
- 0<=A,B,C,D<=255
- 0.0.0.0to 255.255.255.255


bit --»
0
31
Address Range
0
CLASS A ADDRESS
0.0.0.0 – 127.255.255.255
1
0
CLASS B ADDRESS
128.0.0.0 – 191.255.255.255
1
1
0
CLASS C ADDRESS
192.0.0.0 – 223.255.255.255
1
1
1
0
CLASS D ADDRESS
224.0.0.0 – 239.255.255.255
1
1
1
1
0
RESERVED ADDRESS
240.0.0.0 – 247.255.255.255

How to recognized address classes

- 1)for the address 24.46.8.95 identify the type of network and find the network address



Network id

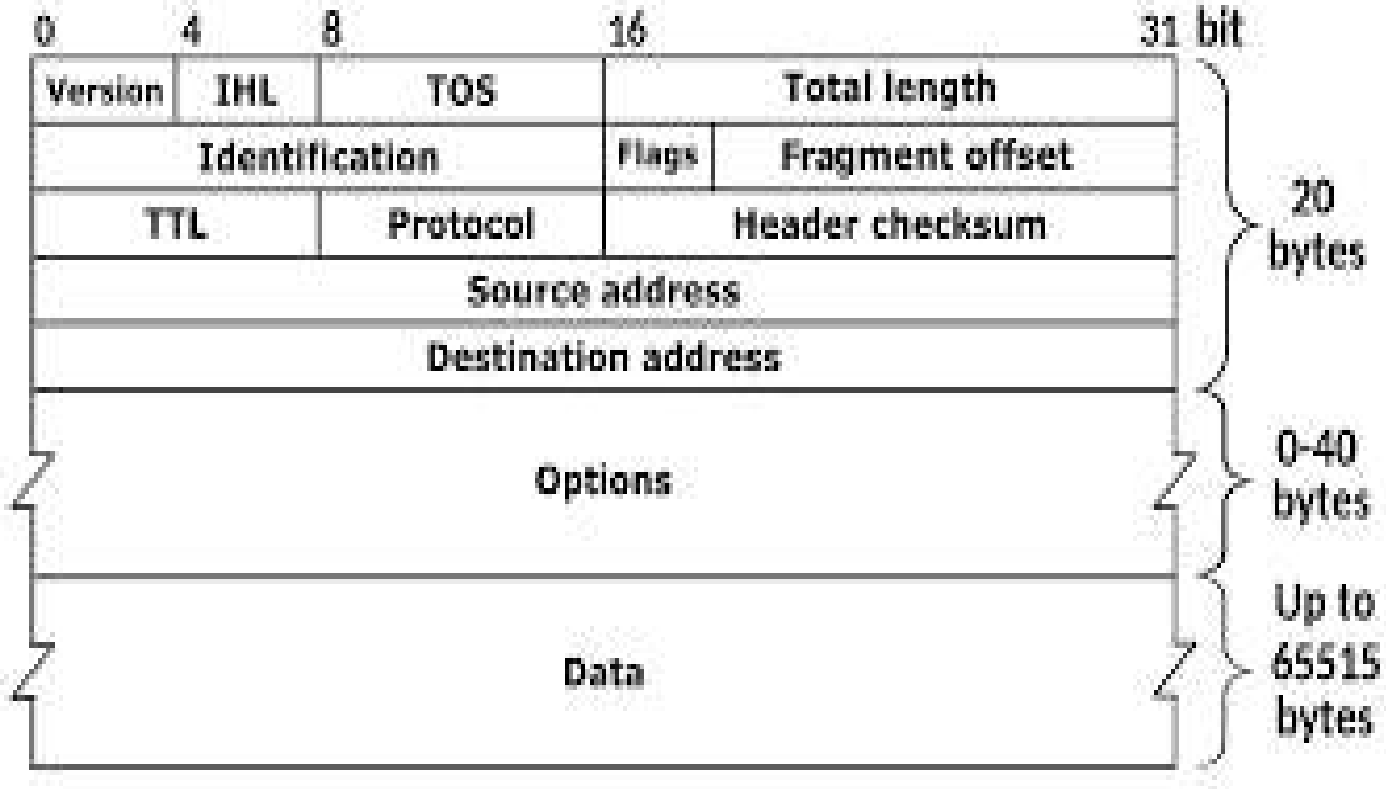
- Class A present in between 0-127 so it is a class A.First byte represent network id it kept as it is & replace host id by zeros.

- 2)for the address 132.7.21.84 identify the type of network and find the network address

- 3)for the address 221.46.75.64 identify the type of network and find the network address

- Valid IP address:
- 10.10.56.80
- 240.230.220.89
- 1.2.3.4
- 99.88.67.89
- 100.200.150.90
- Invalid IP address
- 56.89.1.2.5
- 10.055.34.56
- 200.28.256.8

IPv4 Header


0
4
8
16
31
bit
Version
IHL
TOS
Total length
Identification
Flags
Fragment offset
TTL
Protocol
Header checksum
Source address
Destination address
Options
Data
20 bytes
0-40 bytes
Up to 65515 bytes

- 1)version: this field defines the version of IP protocal.it is 4th but now available in IPv6
- 2)HLN(header length): define the length of the datagram header in 4 byte.
- 3)service type:It defines how the datagram should be handled.possible services such as
- Low delay,high throughput
- 4)Total length: define the total length of IP datagram. 2^16 =65535 bytes
- 5)Identification:used to identify datagram originating from source host.
- 6)flags

Fragmented bit	Not fragmented bit	reserved

7)Fragment offset:consist of relative fragment offset address

- 8)TTL (time to live)
- Denotes total number of router visited by datagram during its life time.
- 9)Protocol:denotes higher level protocol which uses services of IP layer
- This protocol encapsulated in IP datagram those are UDP,TCP,ICMP,IGMP
- 10)header checksum: checksum is updated on each point that the internet header is processed
- 11)source address:
- 12)destination address

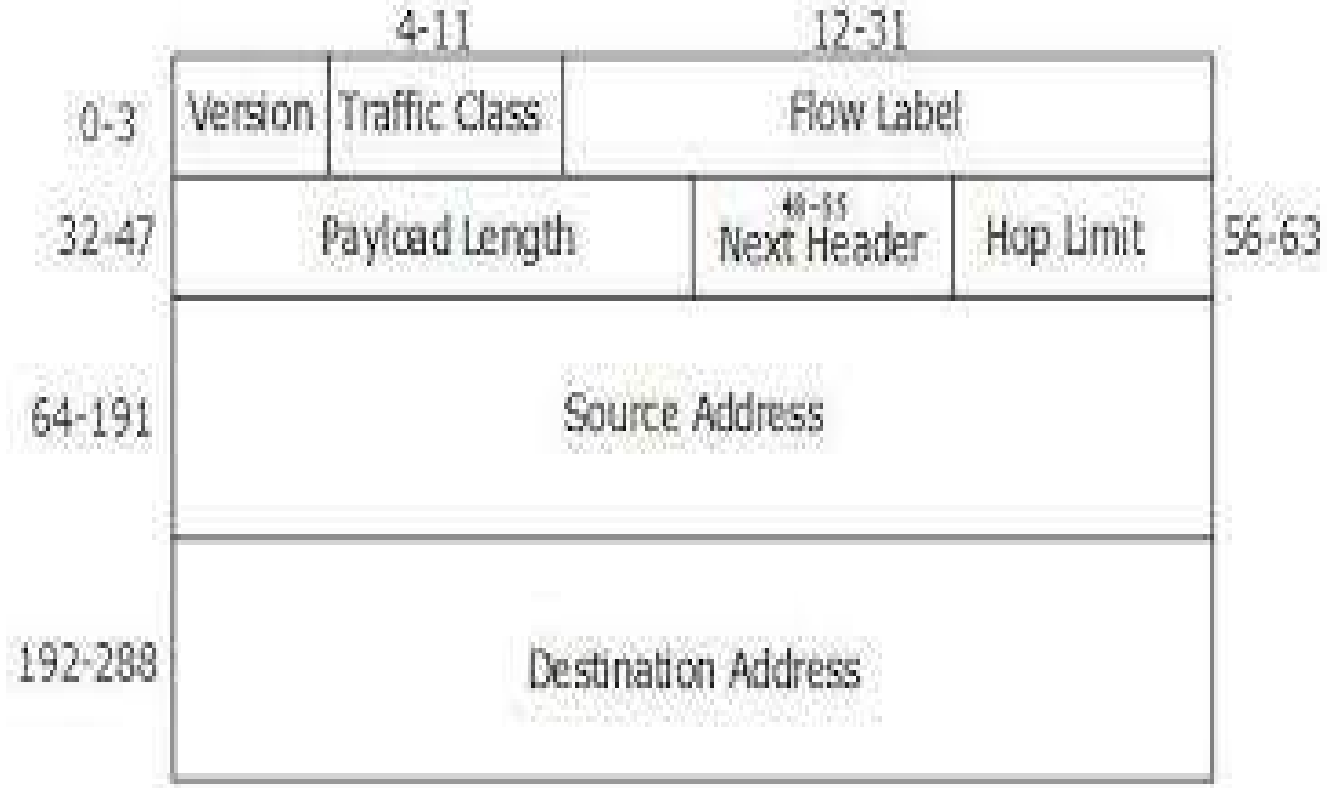
IPv6

- IPv6 is next generation protocol.
- Used to work with IOT
- Connect multiple home appliance with internet (TV,bulb,washing machine,AC)
- Limitaion of IPv4 is that it is 32 bit so 2^32 address are not sufficient to configure the host .
- IPv6 consist of 2^128=3.40,282,366,920… it is more IP address to configure the host.

Advantages of IPv6

- Real time data transmission
- Authentication
- Encryption
- fast processing in route

IPv6 header


4-11
12-31
0-3
Version
Traffic Class
Flow Label
32-47
Payload Length
48-55
Next Header
Hop Limit
56-63
64-191
Source Address
192-288
Destination Address

- 1)version:defines the version of IP protocol i.e IPv6
- 2)priority:shows priority of packets
- 3)flow label :convert datagram into virtual circuits so packet send in one line.
- 4)payload length:send lengthy packets.
- 5)next reader:optional
- 6)HOP limit:decide packet is send to how many host

Network layer consist of 3 protocol

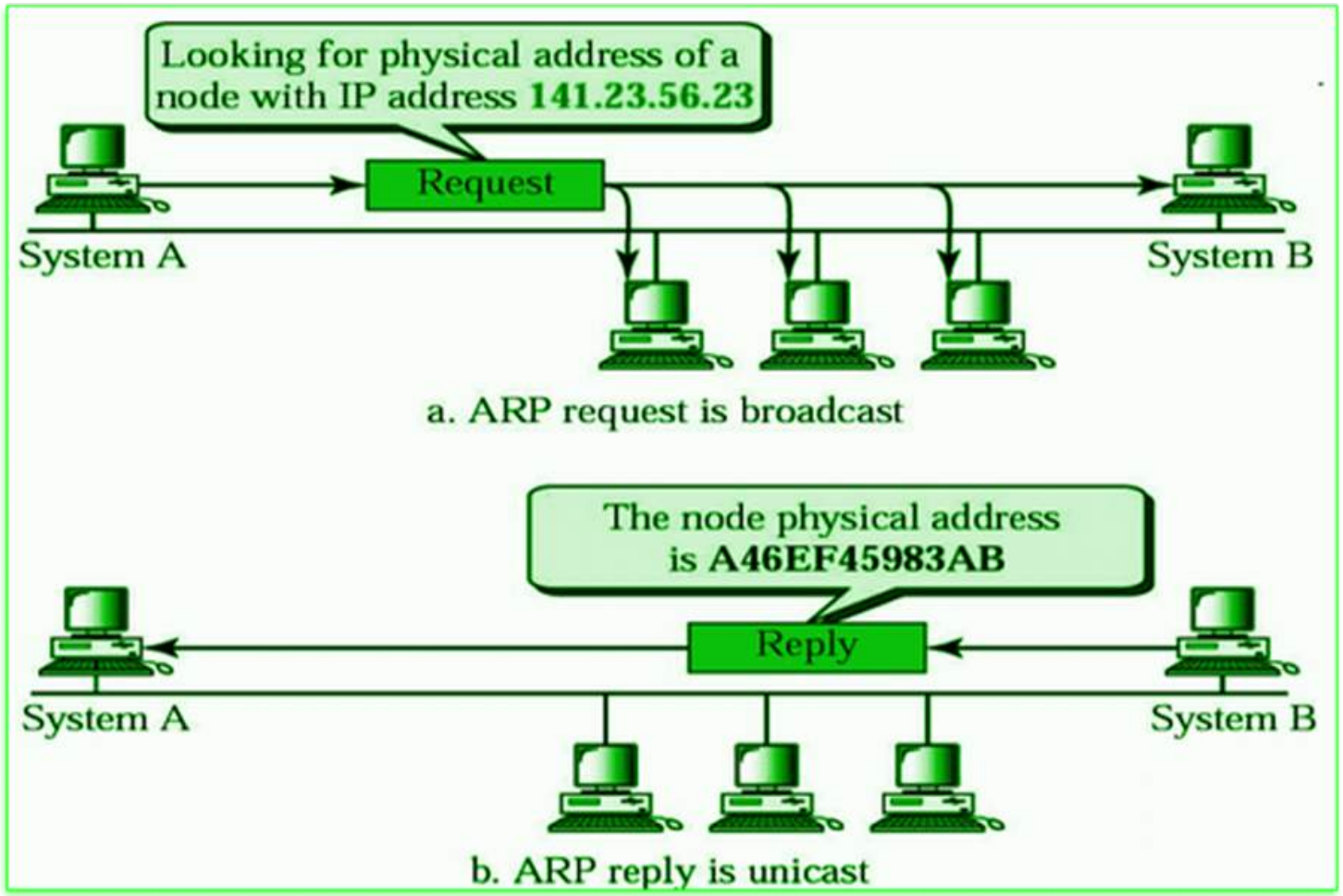
- 1)IP
- 2)ICMP
- 3)IGMP

ICMP4(internet control message protocol)

- IPv4 do not report the error.

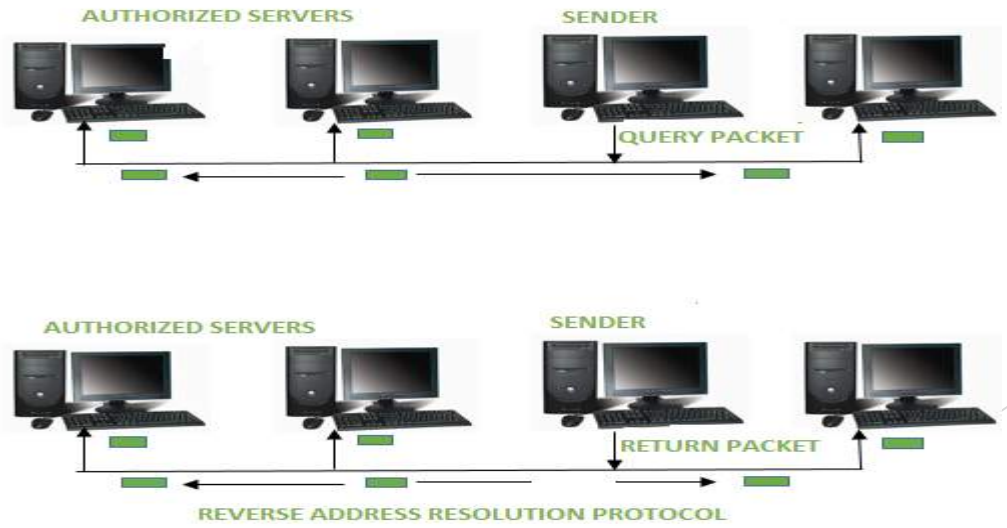
N/W Layer Protocols :ARP

- **1)ARP (Address Resolution Protocol)**
- ARP stands for Address Resolution Protocol.
- ARP is used to convert the logical address ie. IP address into physical address ie. MAC address.
- While communicating with other nodes, it is necessary to know the MAC address or physical address of the destination node.
- If any of the node in a network wants to know the physical address of another node in the same network,
- the host then sends an ARP query packet. This ARP query packet consists of IP address and MAC address of source host and only the IP address of destination host.
- This ARP packet is then received to every node present in the network. The node with its own IP address recognizes it and sends it MAC address to the requesting node.


Looking for physical address of a node with IP address 141.23.56.23
Request
System A
System B
a. ARP request is broadcast
The node physical address is A46EF45983AB
Reply
System A
System B
b. ARP reply is unicast

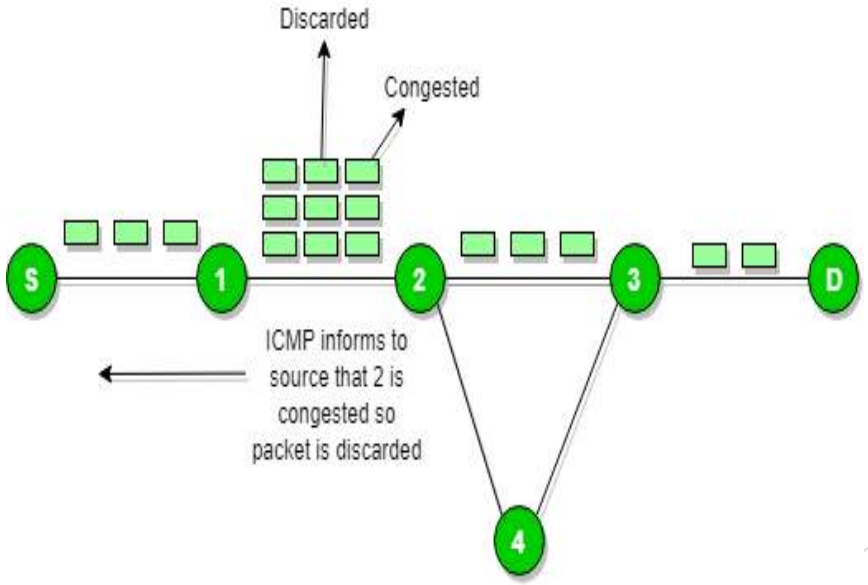
2)RARP

- RARP stands for **Reverse Address Resolution Protocol.**
- RARP works opposite of ARP.
- **Reverse Address Resolution Protocol is used to convert MAC address ie. physical address into IP address ie. logical address.**
- RARP provides with a feature for the systems and applications to get their own IP address from a DNS(Domain Name System) or router.



3)ICMP

- ICMP stands for **Internet Control Message Protocol**.
- ICMP is a part of IP protocol suite.
- ICMP is an **error reporting and network diagnostic protocol.**
- Feedback in the network is reported to the designated host.
- Meanwhile, if any kind of error occur it is then reported to ICMP. ICMP protocol consists of many error reporting and diagnostic messages.

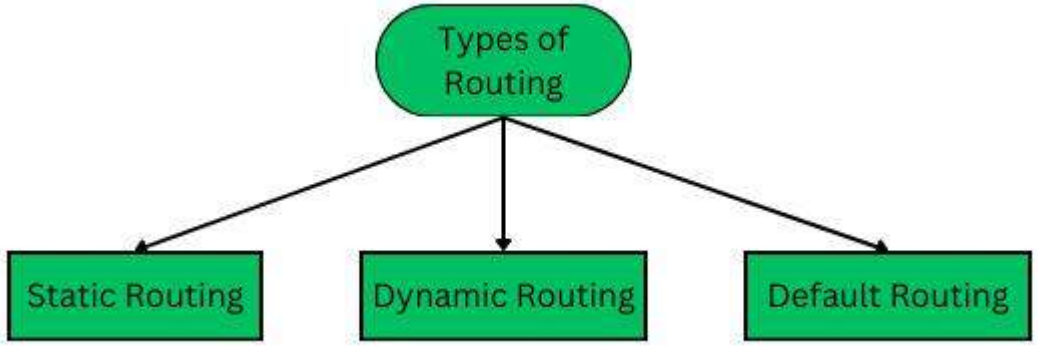


4)IGMP

- IGMP stands for **Internet Group Message Protocol.**
- IGMP is a **multicasting communication protocol.**
- **It utilizes the resources efficiently while broadcasting the messages and data packets.**
- Other **hosts connected in the network and routers makes use of IGMP for multicasting communication.**
- In many networks multicast routers are used in order to transmit the messages to all the nodes.
- Multicast routers therefore receives large number of packets that needs to be sent. But to broadcast this packets is difficult as it would increase the overall network load. Therefore IGMP helps the multicast routers by addressing them while broadcasting

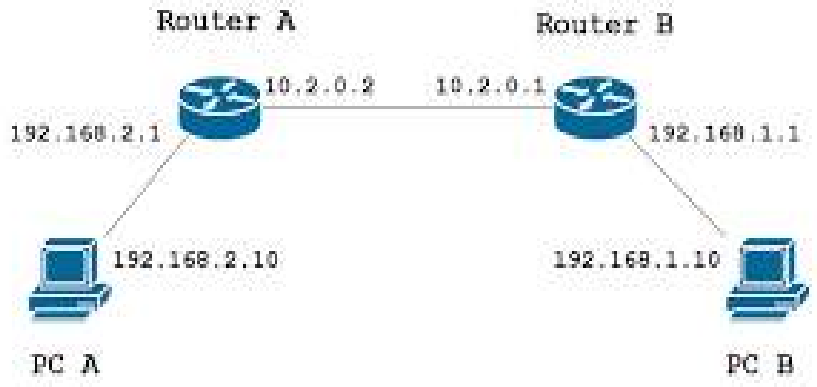
Routing Algorithms

- **What is Routing?**
- Routing is a **process that is performed by network layer**
- It **deliver the packet by choosing an optimal path from one network to another.**
- The **node here refers called – "Router".**
- Routing is a crucial mechanism that transmits data from one location to another across a network (Network type could be any like LAN, WAN, or MAN).



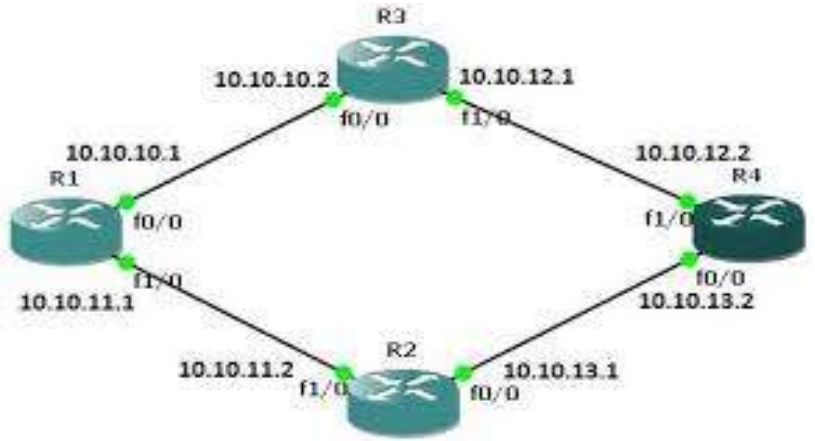
1. Static Routing

- Static routing is also called as “non-adaptive routing”.
- In this, **routing configuration is done manually by the network administrator.**
- Let’s say for example, **we have 5 different routes to transmit data from one node to another, so the network administrator will have to manually enter the routing information by assessing all the routes.**



2.Dynamic Routing

- Dynamic routing is also known as **adaptive** routing which changes the routing table according to the change in topology.
- Dynamic routing uses complex routing algorithms and it does not provide high security like static routing.
- When the network change(topology) occurs, it sends the message to the router to ensure that changes then the routes are recalculated for sending updated routing information.

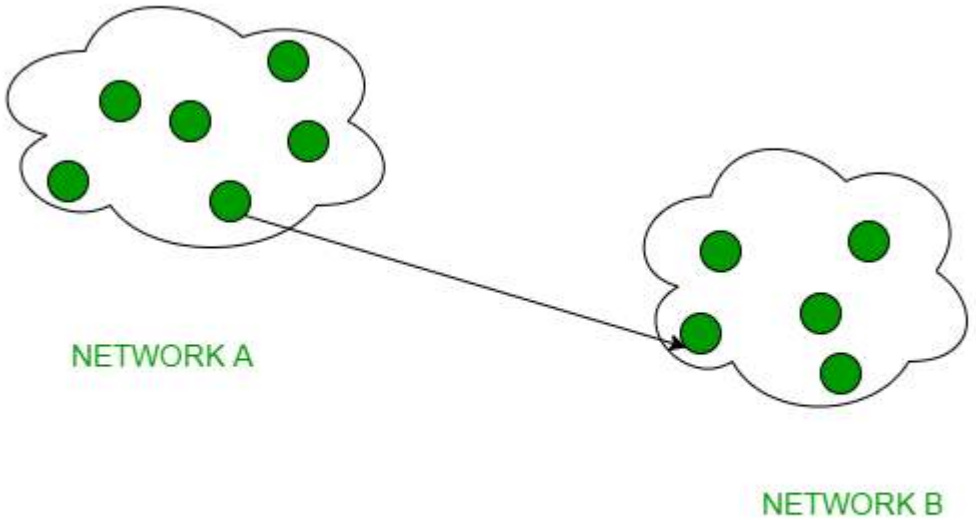


- **Major Protocols of Unicast Routing**
- Unicast means the transmission from a single sender to a single receiver. It is a point-to-point communication between the sender and receiver. There are various unicast protocols such as TCP, HTTP, etc.

1)Distance Vector Routing:

2)Link-State Routing:

3)Path-Vector Routing:



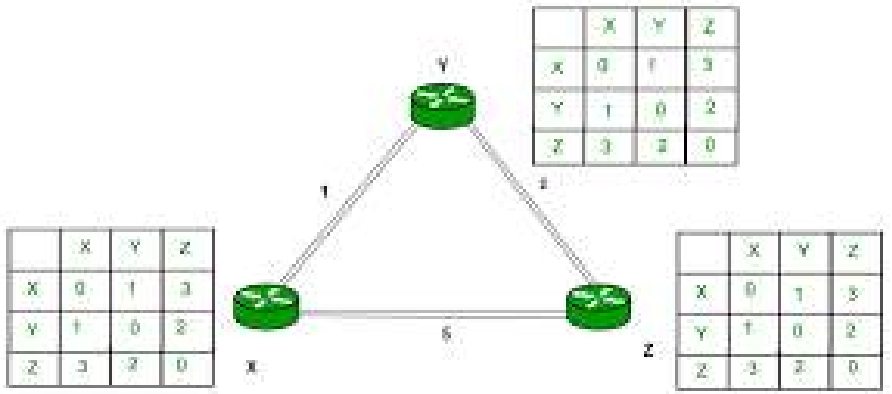
UNICAST EXAMPLE

1)Distance Vector Routing (DVR) Protocol

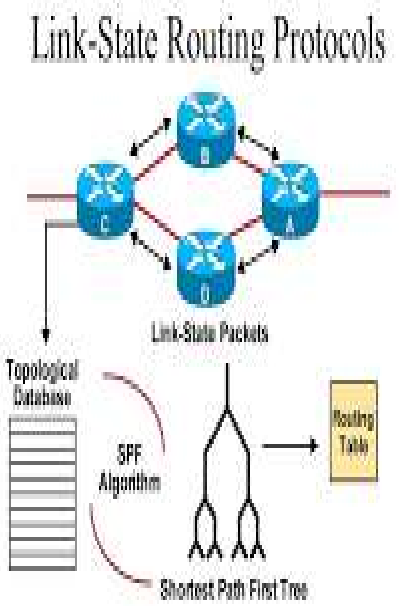
- Distance Vector Routing (DVR) Protocol is a method used by routers to find the best path for data to travel across a network.
- Each router keeps a table that shows the shortest distance to every other router,
- based on the number of hops (or steps) needed to reach them.
- Routers share this information with their neighbors, allowing them to update their tables and find the most efficient routes.
- This protocol helps ensure that data moves quickly and smoothly through the network.

How it works

- A router transmits its distance vector to each of its neighbors in a routing packet.
- Each router receives and saves the most recently received distance vector from each of its neighbors.
- A router recalculates its distance vector when:
  - It receives a distance vector from a neighbor containing different information than before.
  - It discovers that a link to a neighbor has gone down.



2)Link State Routing



- link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology. Based on this learned topology, each router is then able to compute its routing table by using the shortest path computation.
- **The three keys to understand the link state routing algorithm.**
- **Knowledge about the neighborhood**: a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.
- **Flooding:** Each router sends the information to every other router on the internetwork except its neighbors. This process is known as flooding. Every router that receives the packet sends the copies to all the neighbors. Finally each and every router receives a copy of the same information.
- **Information Sharing**: A router send the information to every other router only when the change occurs in the information.

Routing Protocols:1)Routing Information Protocol

2)Routing Protocol:OSPF

3)Routing Protocol:BGP

4)Routing Protocol:MPLS