

Module 1

Introduction to Computer Networks



Dr. Sunandita Debnath, IIIT Vadodara

Evaluation Policy

Evaluation Breakdown

1. Mid-Term Assessment - 30%

- a. Pre-Mid-Sem Examination (10%)
- b. Online Mid-Sem Examination (10%)
- c. Remote Mid-Sem Examination (10%)

2. End-Term Assessment – 45%

- a. Pre-End-Sem Examination (15%)
- b. Online End-Sem Examination (15%)
- c. Remote End-Sem Examination (15%)

3. Other components (Assignments, Quizzes and Viva) - 25%

Course Content of Computer Networks

MODULE 1

Overview of an internet, internet as a service, internet architecture, circuit switching, packet switching, network performance metrics (delay, packet loss, and throughput), layered approach (TCP/IP and OSI models)

Course Instructor

Dr. Sunandita Debnath

Assistant Professor, IIIT Vadodara

Contact No. 9508370853, WhatsApp No. 9485145373

Google classroom Code: d3w7vqi

Reference Books

1. Computer Networking: A Top-Down Approach (Fifth Ed. by J. F. Kurose and K. W. Ross, publisher: Pearson)
2. Data Communications and Networking (Fourth Ed. by B. A. Forouzan, publisher: McGraw Hill Education)
3. Computer Networks (Fifth Ed. by A. S. Tanenbaum and D. J. Wetherall, publisher: Pearson)

What is Internet?

The internet is a computer network that interconnects zillions of computing devices throughout the world.

“Internet is a network of networks”

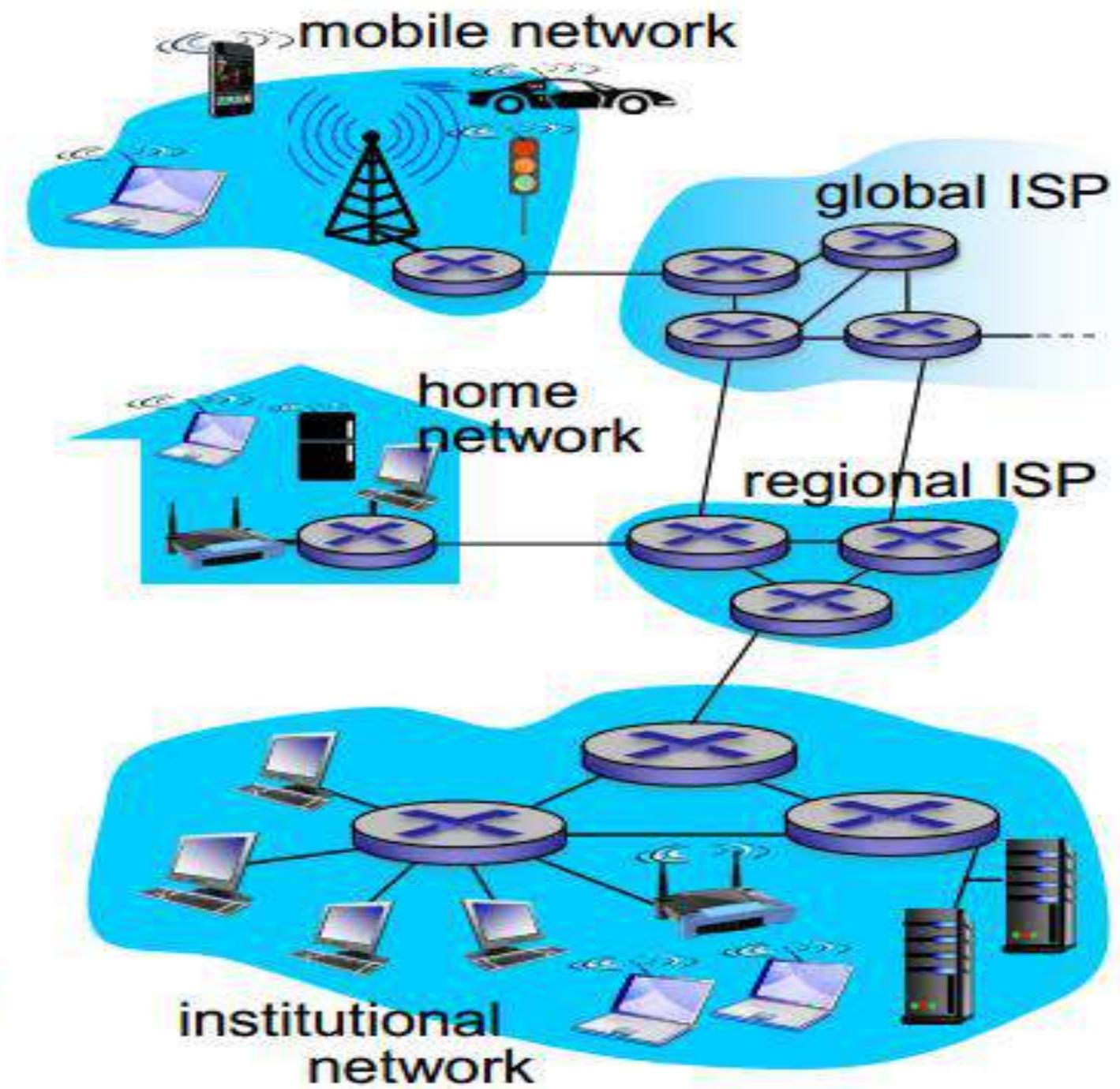
Computer networks

- A computer network is a set of nodes or specifically end systems connected by communication links .
- Three important terms in computer networking is:
- *Nodes*
- *Communication links*
- *Packet switches*

“Internet is everywhere”

Application includes:

- *Electronics mail*
- *Web surfing*
- *Social networks*
- *Instant Messaging*
- *Voice over IP (VoIP)*
- *Distributed games*
- *Peer-to-peer*
- *File sharing*
- *Television over internet*
- *Remote login*



Nodes

End Nodes/Host

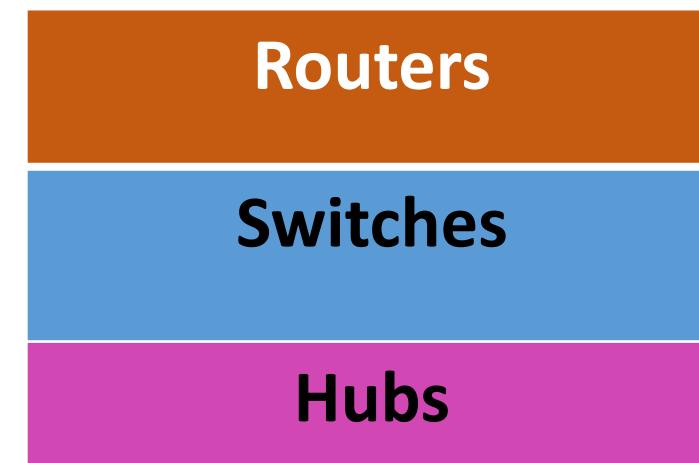
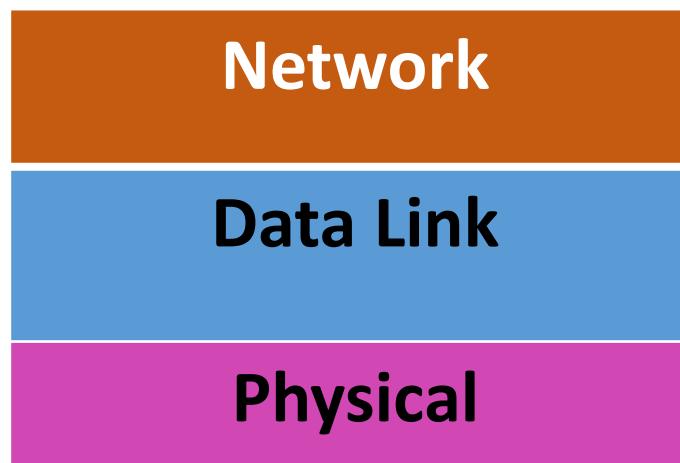
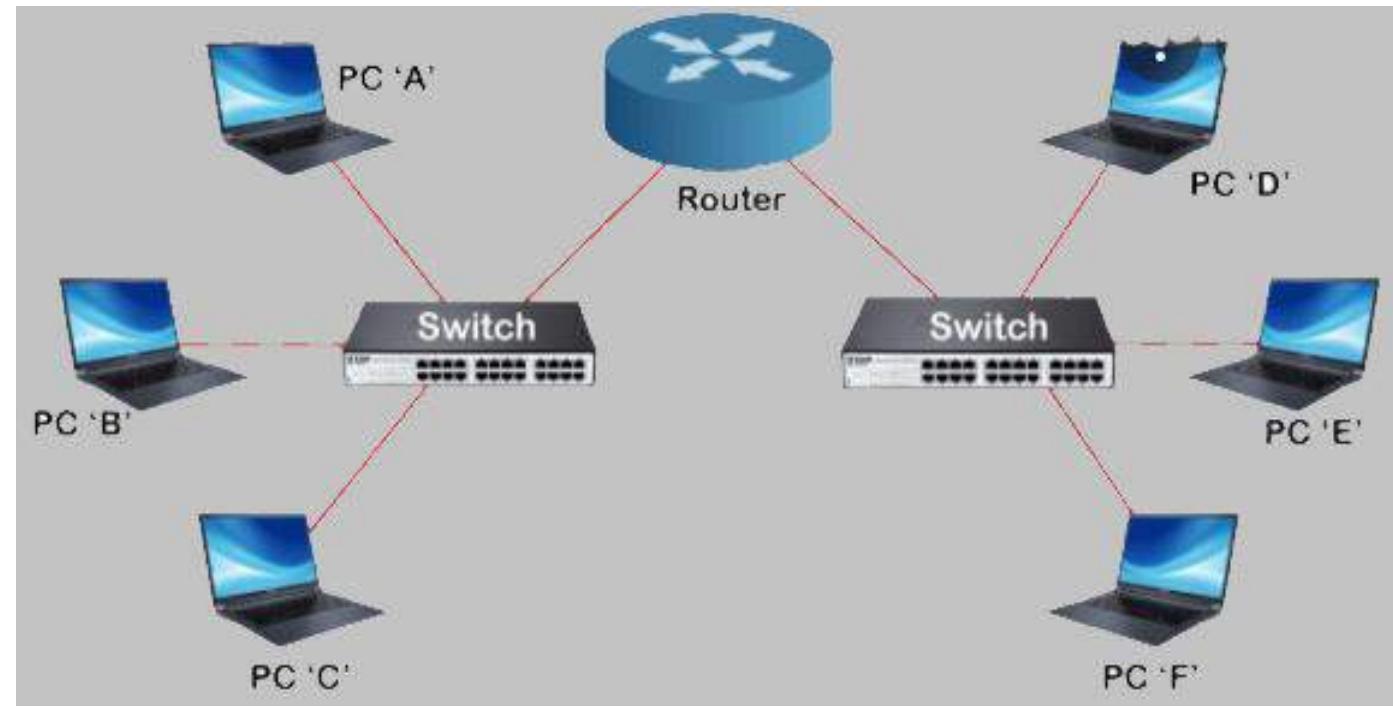
A end node can be a computer, printer, mobile phones, PDAs (Personal Digital Assistants) or any other devices capable of sending/ receiving data generated by the other nodes in the network.



Intermediary nodes:

A intermediary node can be a hub, cell phone tower, repeaters, routers, switches etc.

- **Important terms in computer networking is:**
- *Hosts/End users*
- *Communication links (Wired or Wireless)*
- *Routers*
- *Switches*
- *Hub*
- *Servers*
- *Client*



Communication links

A commination link can be wired or wireless links. This link or channel carries information.

- **Co-axial cables, Optical Fiber, and RF spectrum (air)**



Wired Media

- Ethernet straight (for different type of devices)
- Ethernet cross (for same type of devices)
- Co-axial cables
- Optical Fibers
- USB cables



Wireless Media

- Infrared (for short rang e.g. TV/AC remote controls)
- Radio (e.g. Bluetooth, WiFi)
- Microwave links (e.g. Cell phone tower)
- Satellite links (for GPS)



Packet switches

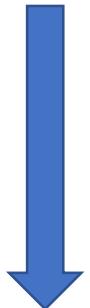
Packet switches receives a packet arriving on one of its incoming communication links and forwards that packet on one of its outgoing communication links.

- **Routers (Core Networks)**
- **Link layer switches (Access Networks)**

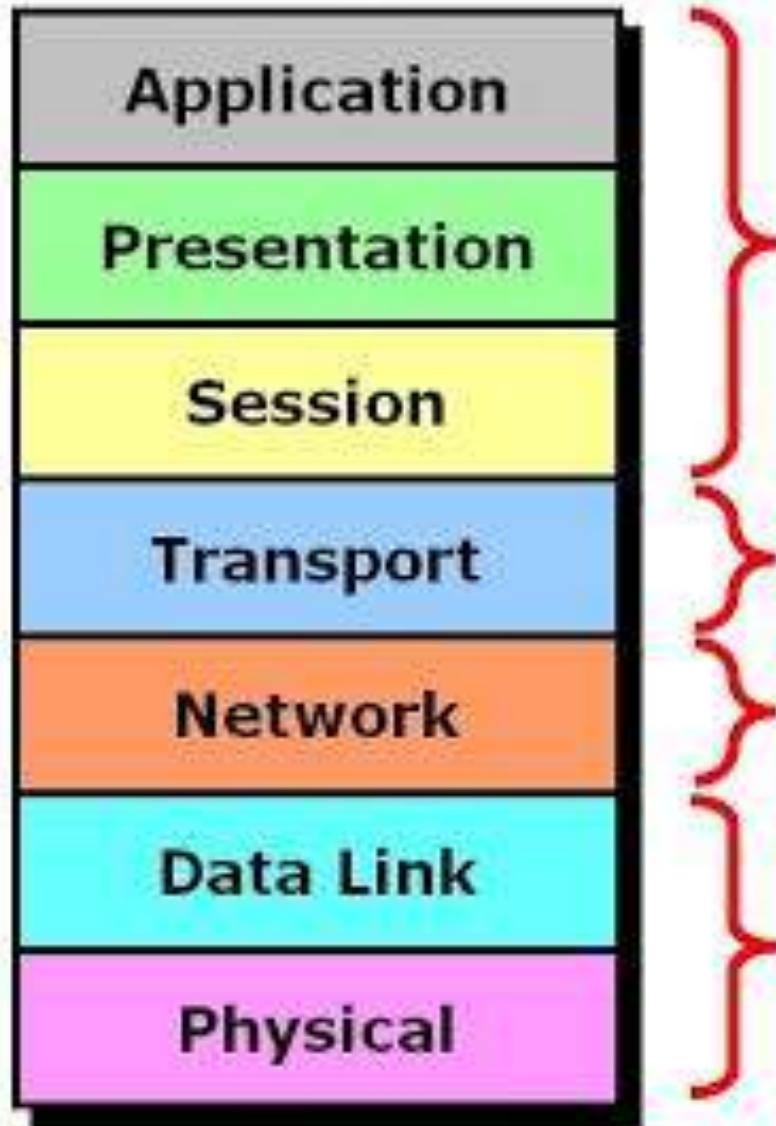
End systems access the internet through ISPs (Internet service providers). ISPs can be different type:

- **Residential ISPs (e.g. Local cables or Telephone companies)**
 - **Corporate ISPs (e.g. Offices)**
 - **University and Colleges ISPSs (IIIT Vadodara)**
 - **ISPs that provides WiFi access in airports, coffee shops and railway stations and other public places**
- ❖ *Each ISP n itself a network of packet switches and communication links.*

Sender



Receiver



OSI Layers

Application

Transport

Network

Data Link

Physical

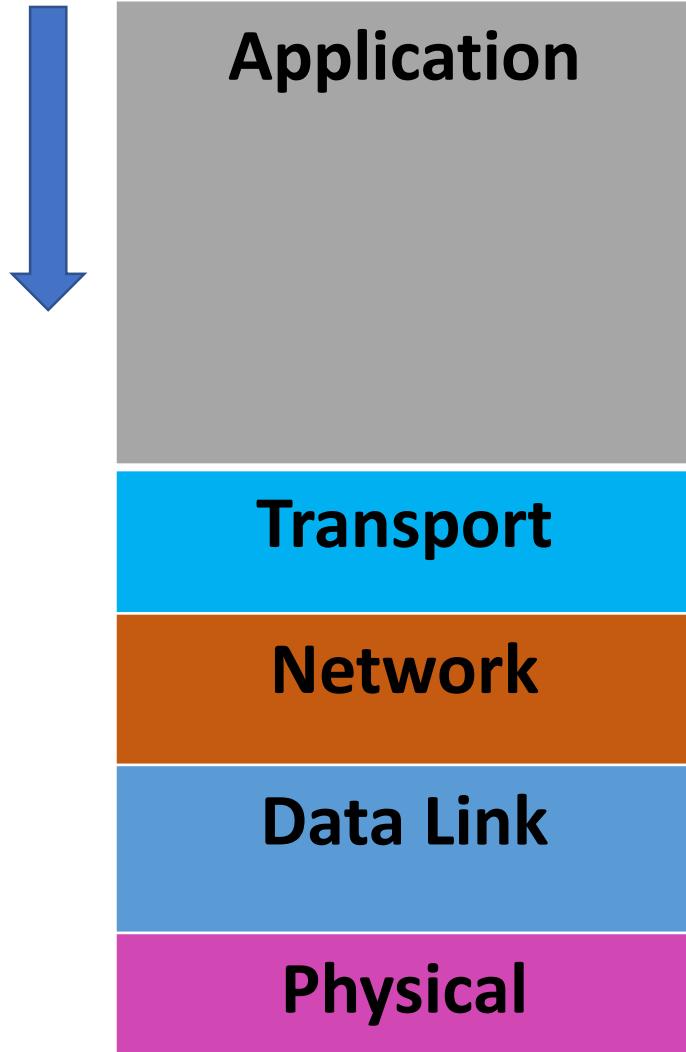
Software
Layers

Heart of OSI

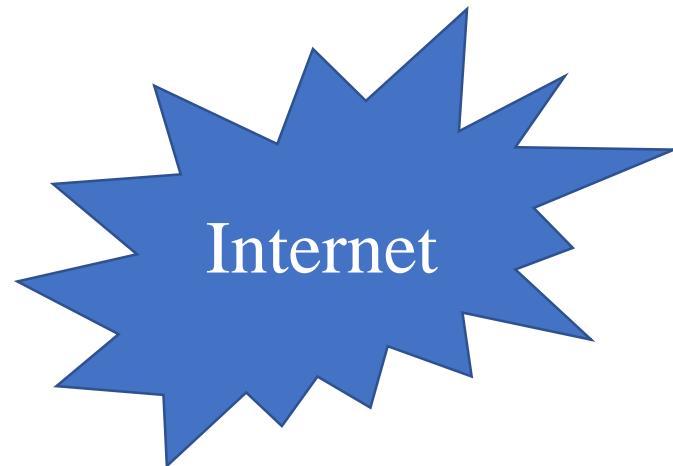
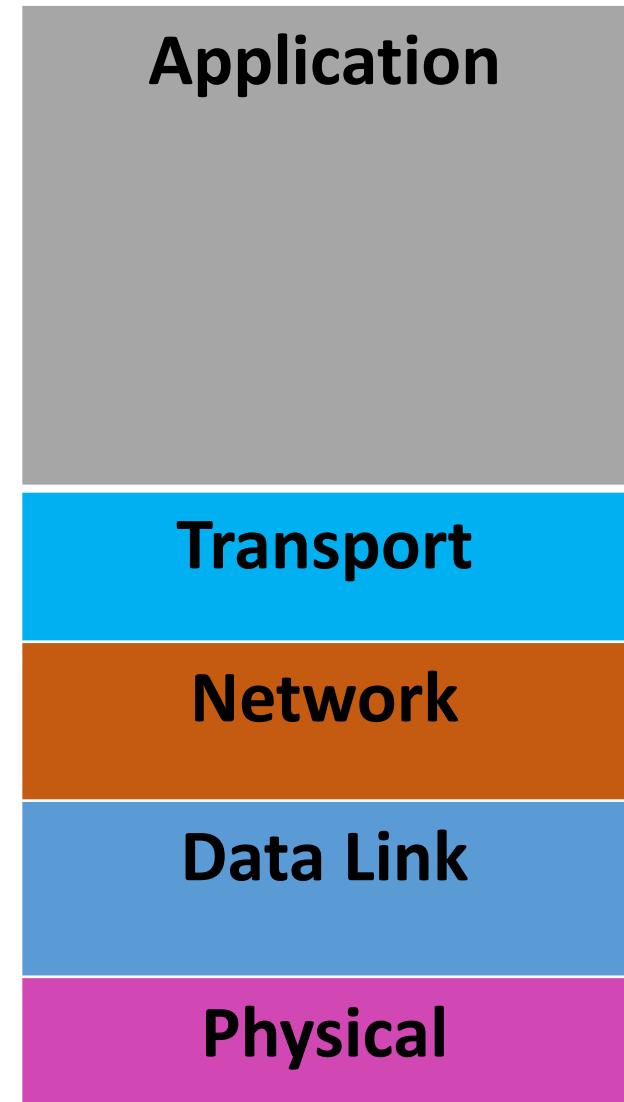
Hardware
Layers

TCP/IP Layers

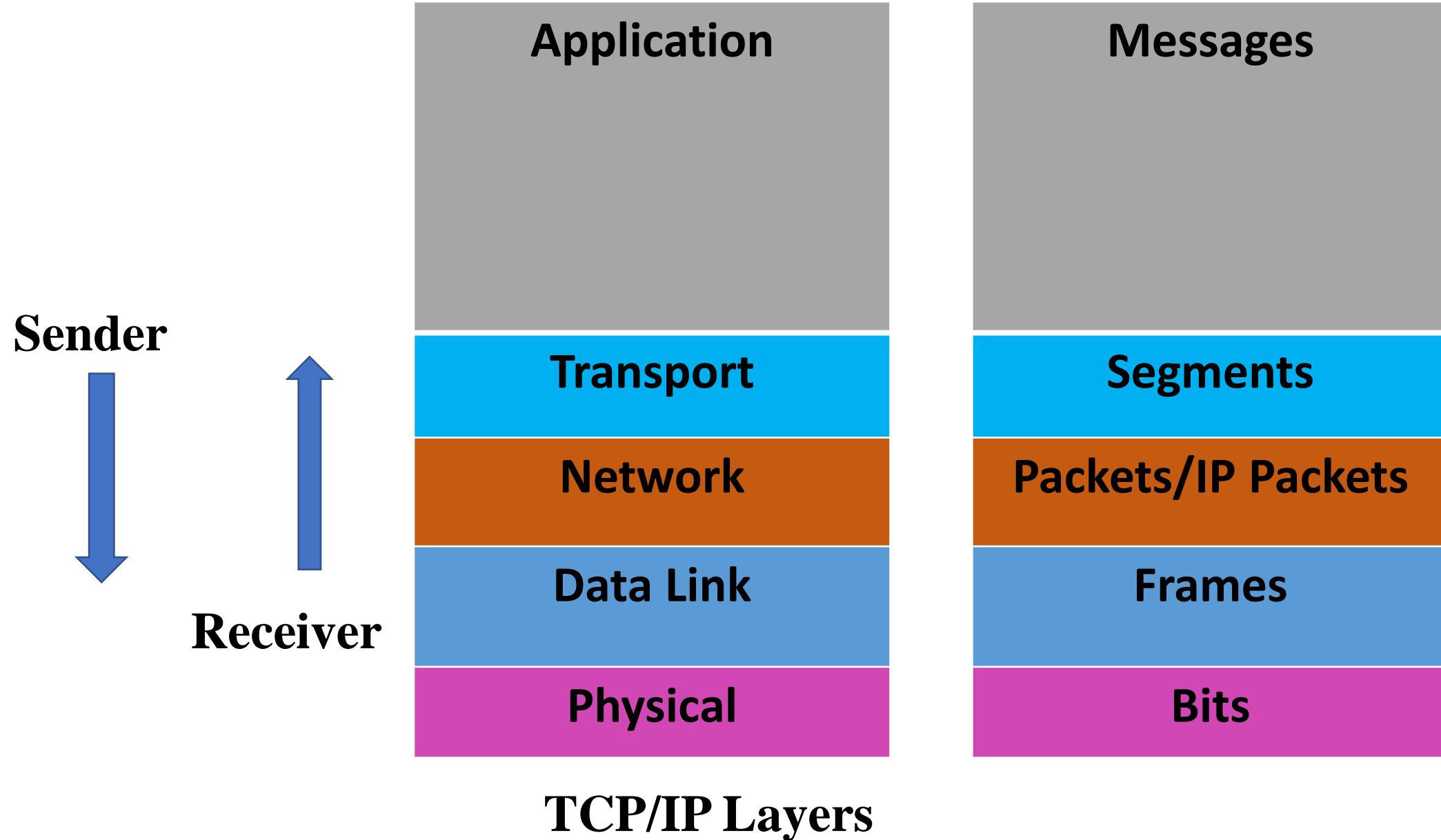
Sender



Receiver



Packet data Units (PDUs)



- **Intermediary Devices**

Network

Data Link

Physical

Routers: Data-Packets, Devices: between Intelligent devices, Full duplex, Addressing Type: IP address, Between two different networks, Routing Device

Switches: frames, Devices: between Intelligent devices, Half/Full duplex, Addressing Type: MAC address, Between devices on same network, Multicasting Device

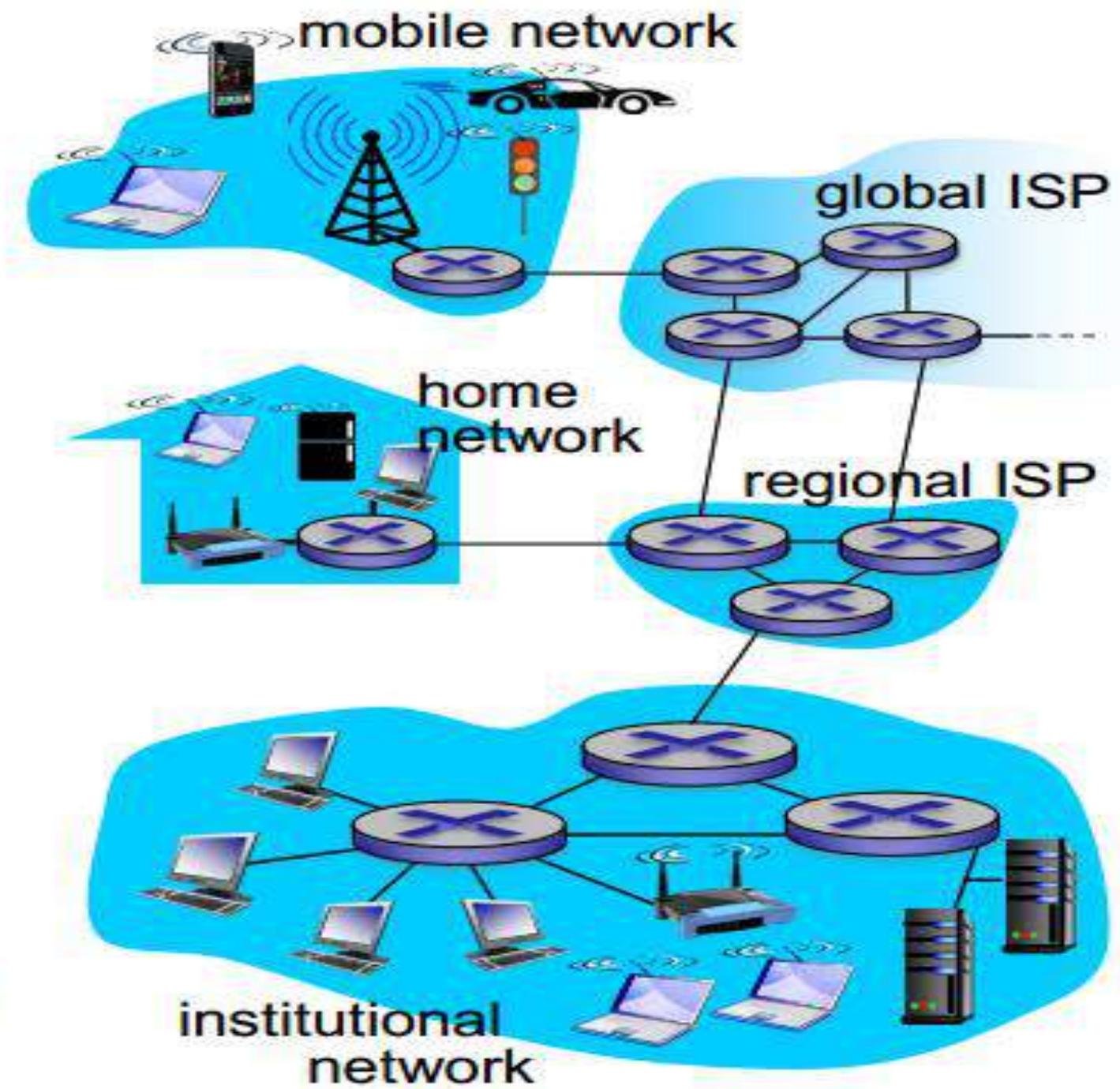
Hubs: Data-Electrical signals/bits, Devices: between Non-intelligent devices, Half duplex, Addressing Type: MAC address, Between devices on same network, Broadcasting device

Module 1

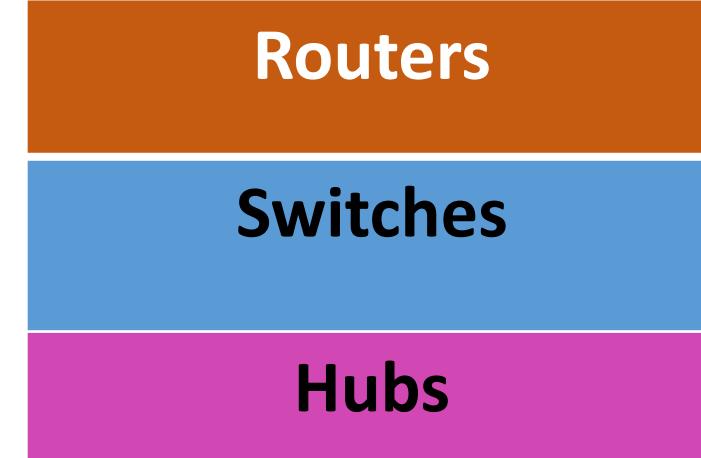
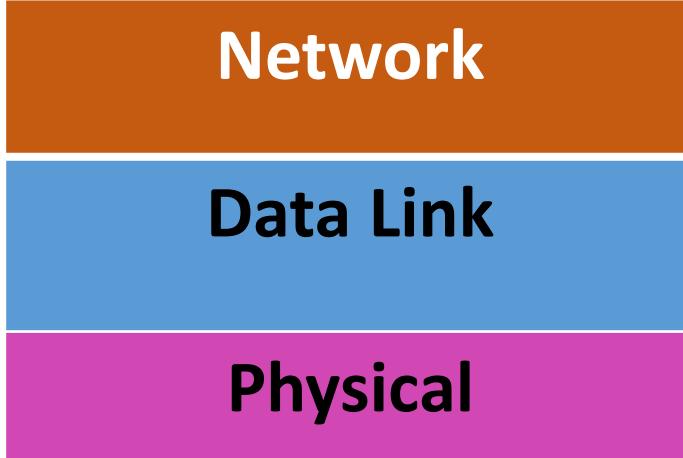
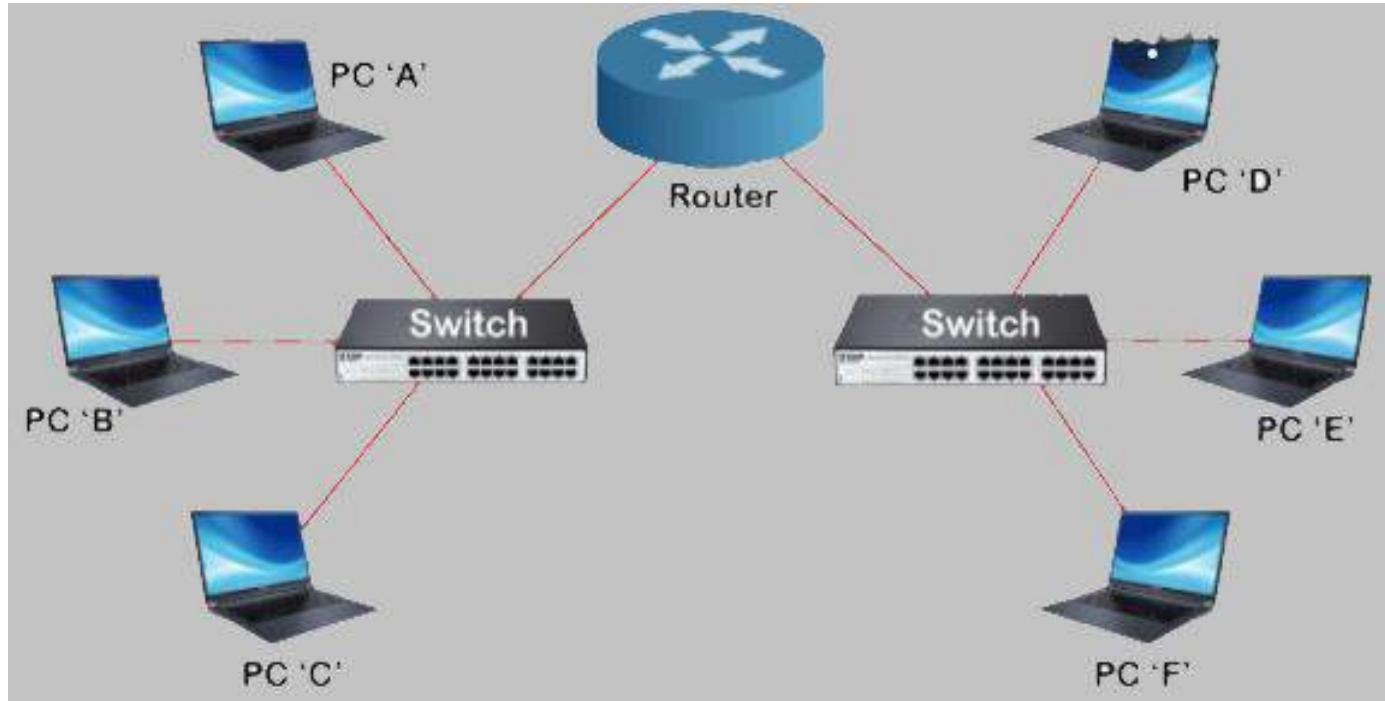
Introduction to Computer Networks



Dr. Sunandita Debnath, IIIT Vadodara



- **Intermediary Devices**
- *Routers*
- *Switches*
- *Hub*



- **Intermediary Devices**

Network

Data Link

Physical

Routers: Data-Packets, Devices: between Intelligent devices, Full duplex, Addressing Type: IP address, Between two different networks, Routing Devices

Switches: frames, Devices: between Intelligent devices, Half/Full duplex, Addressing Type: MAC address, Between devices on same network, Multicasting Device

Hubs: Data-Electrical signals/bits, Devices: between Non-intelligent devices, Half duplex, Addressing Type: MAC address, Between devices on same network, Broadcasting device

Communication links

A commination link can be wired or wireless links. This link or channel carries information.

- **Co-axial cables, Optical Fiber, and RF spectrum (air)**



Wired Media

- Ethernet straight (for different type of devices)
- Ethernet cross (for same type of devices)
- Co-axial cables
- Optical Fibers
- USB cables



Wireless Media

- Infrared (for short rang e.g. TV/AC remote controls)
- Radio (e.g. Bluetooth, WiFi)
- Microwave links (e.g. Cell phone tower)
- Satellite links (for GPS)

Packet switches

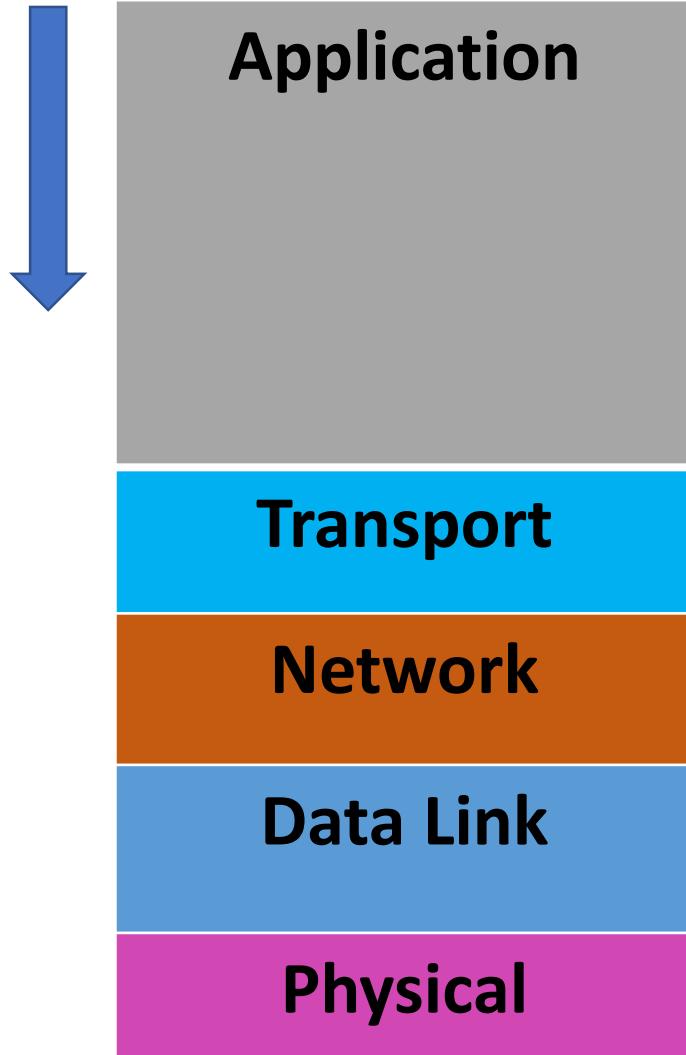
Packet switches receives a packet arriving on one of its incoming communication links and forwards that packet on one of its outgoing communication links.

- **Routers (Core Networks)**
- **Link layer switches (Access Networks)**

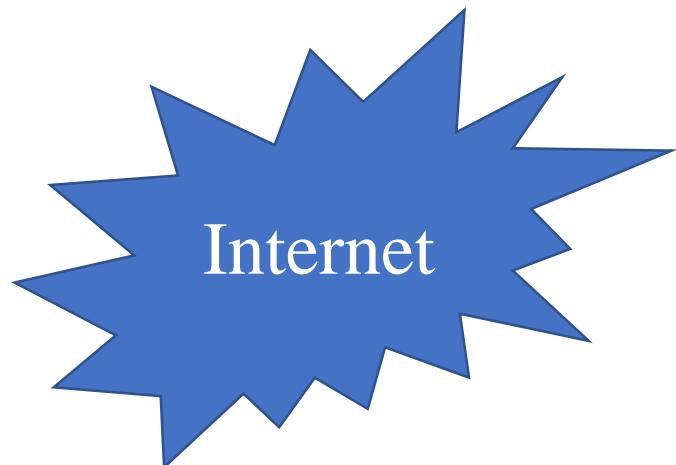
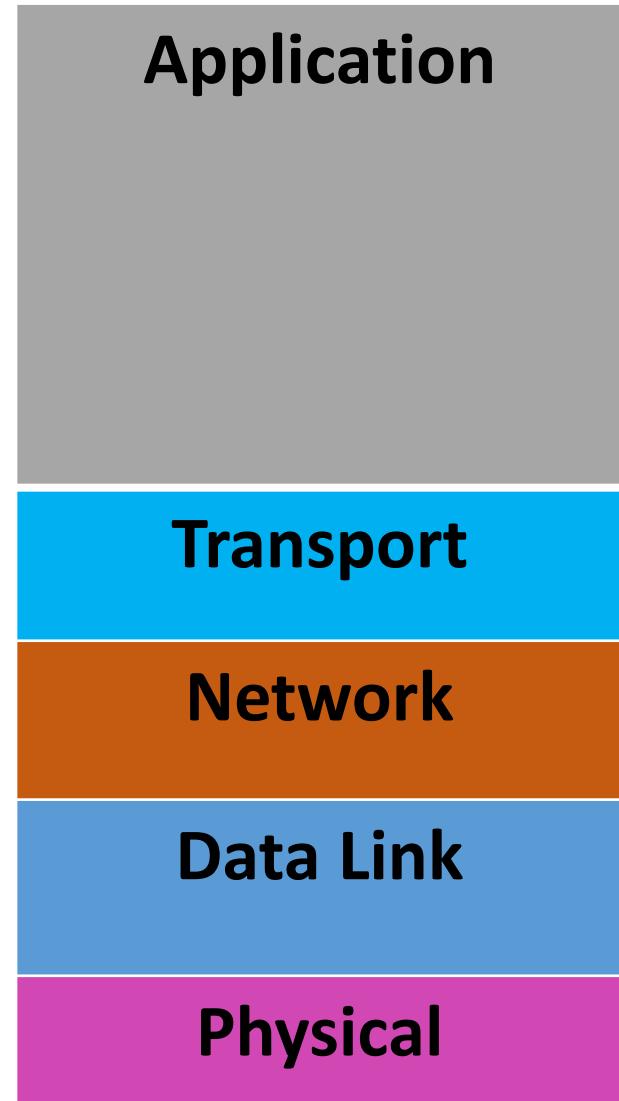
End systems access the internet through ISPs (Internet service providers). ISPs can be different type:

- **Residential ISPs (e.g. Local cables or Telephone companies)**
 - **Corporate ISPs (e.g. Offices)**
 - **University and Colleges ISPSs (IIIT Vadodara)**
 - **ISPs that provides WiFi access in airports, coffee shops and railway stations and other public places**
- ❖ *Each ISP n itself a network of packet switches and communication links.*

Sender



Receiver



Peer to Peer Network

- No centralized administration
- All peers are equal
- Not scalable
- Simple sharing applications

Client server network

- Centralized administration (one will be master and others will be slave)
- Request response model
- Scalable
- Server may be overloaded

Data communication

Data communication is the exchange of data between two nodes via some form of links such as cable.

Data flow in this data communication can be of three types

- Simplex (E.g. Keyboard, Printers etc. one way communication)
- Half-Duplex (E.g. Walkie-Talkies. Two way communication but both not simultaneously)
- Duplex (E.g. Telecommunication. Two way communication at the same time)

Protocols

Protocol is set of rules which governs all types of communication, like

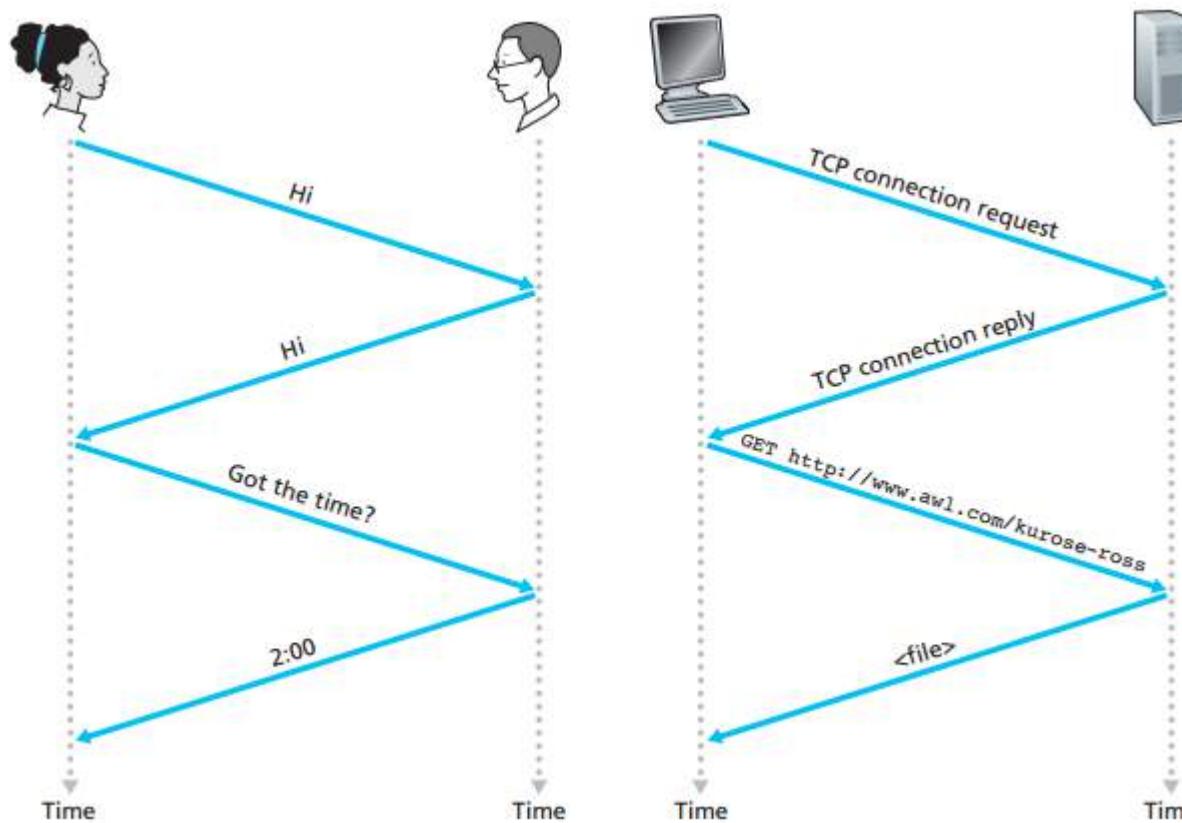
What is communicated?

How it is communicated?

When it is communicated?

Protocol

- This is comparison of a human protocol and computer network protocol



Important points:

- If the system runs two different protocols then the protocols do not inter operate and no useful work can be accomplished.
- The two system should run the same protocol in order to accomplish the task.

- A protocol defines the format and the order of message exchanged between two or more communicating entities, as well as the action taken on the transmission or reception of a message or other event.
- A protocol defines the format and the order of message exchanged between two or more communicating entities, as well as the action taken on the transmission or reception of a message or other event.

Classification of computer networks:

- *LAN (Local Area Network)*
- *MAN (Metropolitan Area Network)*
- *WAN (Wide Area Network)*

Access Network

- The access network is the network or part of communication systems which provide the user access to the internet services.
- Typically connecting devices like phones and laptops to a access point in a café or home network.

Core Network

- The core network is the part of a network that connects different access networks.
- Typically cover wide ranges like network connecting two different cities.

LAN	MAN	WAN
<ul style="list-style-type: none"> <input type="checkbox"/> LAN (Local Area Network) is a computer network covering a small geographic area, like a home, office, school, or group of buildings, University campus. <input type="checkbox"/> High speed (1000 Mbps) <input type="checkbox"/> High bandwidth as lesser number of devices are connected. <input type="checkbox"/> Range can be almost kms. 	<ul style="list-style-type: none"> <input type="checkbox"/> A metropolitan area network (MAN) is a network with a size bigger than a LAN but smaller than a WAN. It normally covers the area inside a town or a city. <input type="checkbox"/> moderate speed(44 to 155 Mbps) <input type="checkbox"/> Less bandwidth than LAN as more devices are connected. <input type="checkbox"/> 100 to 1000 of kms. 	<ul style="list-style-type: none"> <input type="checkbox"/> WAN (Wide Area Network) is a computer network that covers a broad area e.g. country or continent. <input type="checkbox"/> Less speed (150 Mbps) <input type="checkbox"/> Low bandwidth as many MAN are connected. <input type="checkbox"/> Satellite is used to manage WAN.

Module 1

Introduction to Computer Networks



Dr. Sunandita Debnath, IIIT Vadodara

Functions of each layer

Application Layer: *It enables the users to access the network resources. This layer also serves as a window for the application services to access the network and for displaying the received information to the user. It is also called as desktop layer.*

- *Mail services*
- *Directory services*
- *File transfer and Access management*

Protocols: *HTTP, SMTP, FTP, TFTP, DNS, DHCP*

Presentation Layer

It is concerned with the syntax and semantics of the information exchanges between the two systems. It is also called the as translation layer.

- *Translation (converting data into common format)*
- *Encryption (security purpose)*
- *Compression (compressing long duration videos and high resolution images and videos)*

Functions of each layer

Session Layer: *It establishes the connection and maintains the session between the communicating devices. It is also responsible for authentication and security.*

- *Dialog control*
- *Synchronization*
- *Session establishment, maintenance and termination*

Transport Layer: *It is responsible for process-to-process or end-to-end delivery of entire message/data. It provides services to the application layer and takes services from the network layer. This layer is responsible for acknowledgement of successful data transmission and re-transmit the data if error is found. Transport layer adds source and destination port numbers to the segmented data.*

- *Port addressing*
- *Segmentation and reassembly*
- *Connection control*
- *End to end flow control*
- *Error control*

Protocols: *TCP (connection oriented, used for reliable data transmission), UDP (connection less, used for real time traffic)*

Functions of each layer

Network Layer: *It is responsible for delivery of data from original source to destination with the help of IP addresses. It also takes cares of packet routing i.e. selection of the shortest route/path to transmit the packet, from the number of routes available.*

- *Logical addressing*
- *Routing*

Protocols: *ICMP (Internet Control Message Protocol), IPV4/IPV6 (Internet Protocol Version 4, Version 6), RIP (routing Information Protocol)*

Data link Layer: *It is responsible for the node-to-node delivery of frames. The main function of this layer is to make sure that the data transfer is error-free from one node to other, over the physical layer. This layer is divided into LLC(Logical Link Control) and MAC (Media Access Control).*

- *Framing*
- *Physical addressing*
- *Flow control*
- *Error control*
- *Access control*

Protocols: *LLDP, PPP (Point-to-Point), Spanning tree protocol*

Functions of each layer

Physical Layer: *It is responsible for the actual physical connection between the devices , the information are in form of bits. It also provides electrical and mechanical specifications.*

- *Physical characteristics of the medium (either wired or wireless)*
- *Synchronization of bits*
- *Bit rate control*
- *Physical topologies (star, bus or mesh connection)*
- *Transmission mode (duplex, half duplex, full duplex)*

IP Address

- Every node in the computer network is identified with the help of IP address or logical address.
- Can change based on the location of the device
- Assigned manually or dynamically.
- Represented in decimal and it has 4 octets (x.x.x.x).
- 0.0.0.0 to 255.255.255.255. (each octet is represented by 8 bit representation) total 32 bits long.
- Routers need IP address to forward data

MAC Address

- Every node in LAN is identified with the help of MAC address.
- Physical address or hardware address imprinted in the NIC (*Network Interface Controller*) card of the device.
- Cannot be changed it is a unique number, assigned by the manufacturer of the device.
- Represented in Hexadecimal.
- E.g. 70-20-84-00-ED-FC (48bits)
- Separated by, hyphen (-), dot(.), colon (:).
- Switches need MAC address to forward data.

Module 1

Introduction to Computer Networks



Dr. Sunandita Debnath, IIIT Vadodara

Network structure

Network Edge

- *Access Networks*
- *Physical Media*

Network core

- *Packet switching*
- *Circuit Switching*

Network structure

Access Networks-*The network that physically connects an end system to the first router (also known as edge router) on a path from the end system to any other distant end system.*

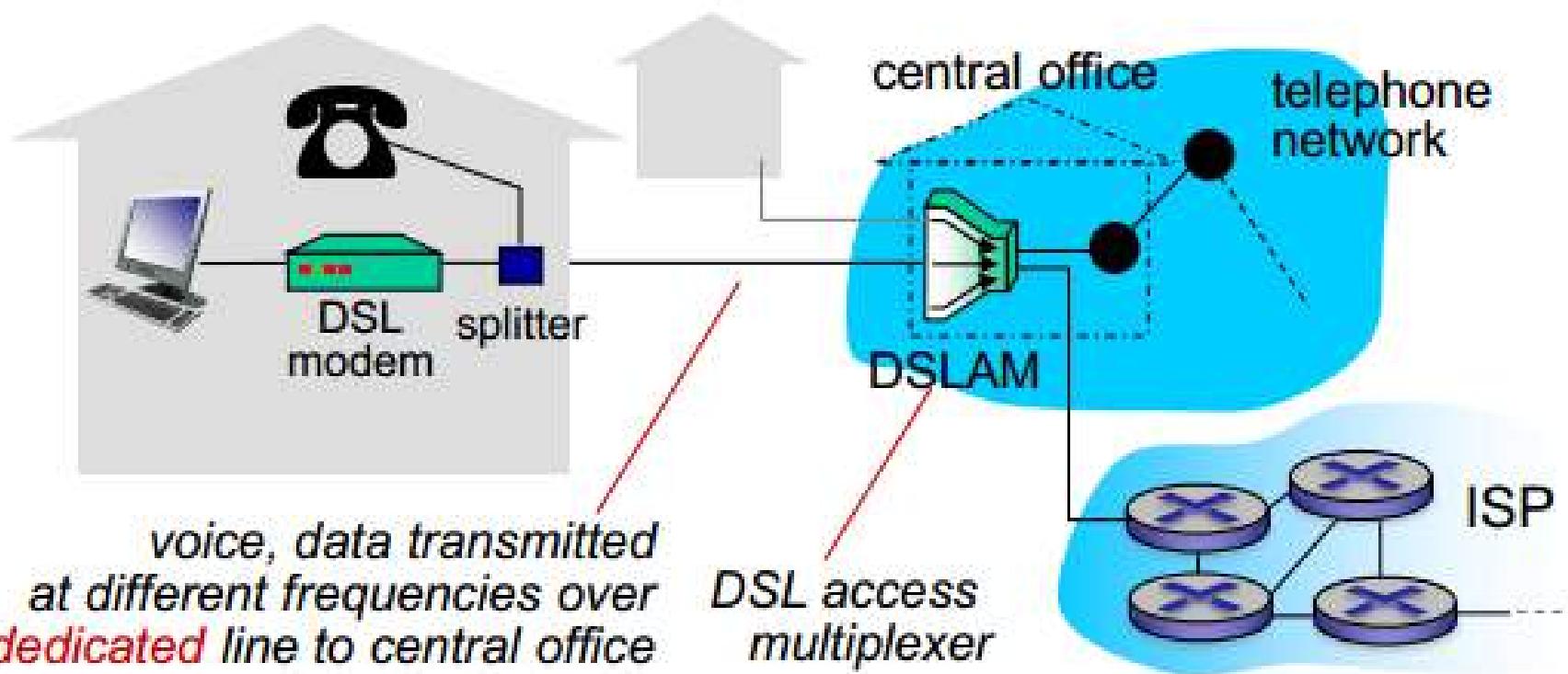
There are three types of access networks

- Home access***
- Enterprise access***
- Wide area mobile wireless***

Home Access structure

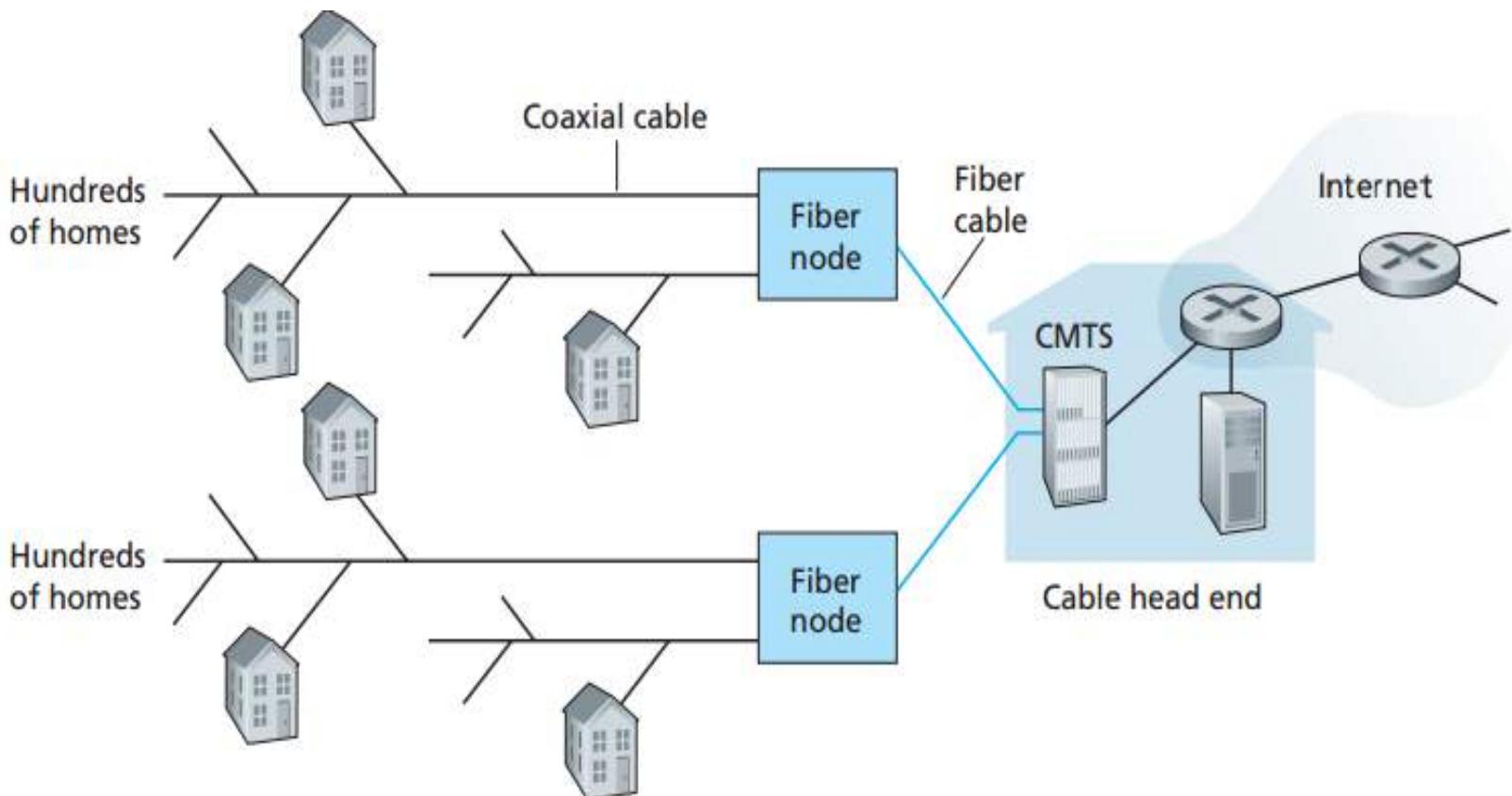
- *DSL (Digital subscriber line), Cable, FTTH (Fiber to the Home), Dial-Up*
- *Each customer's DSL modem uses the existing telephone line (twisted wire) to exchange data with a DSLAM located in the telecom Central Office (CO).*
- *The home's DSL modem takes digital data and translates it to high frequency tones for transmission over telephone wires to CO.*

voice, data transmitted at different frequencies over dedicated line to central office
- *The analog signal from many such houses are translated back into digital format at the DSLAM.*



A Hybrid Fiber co-axial access network

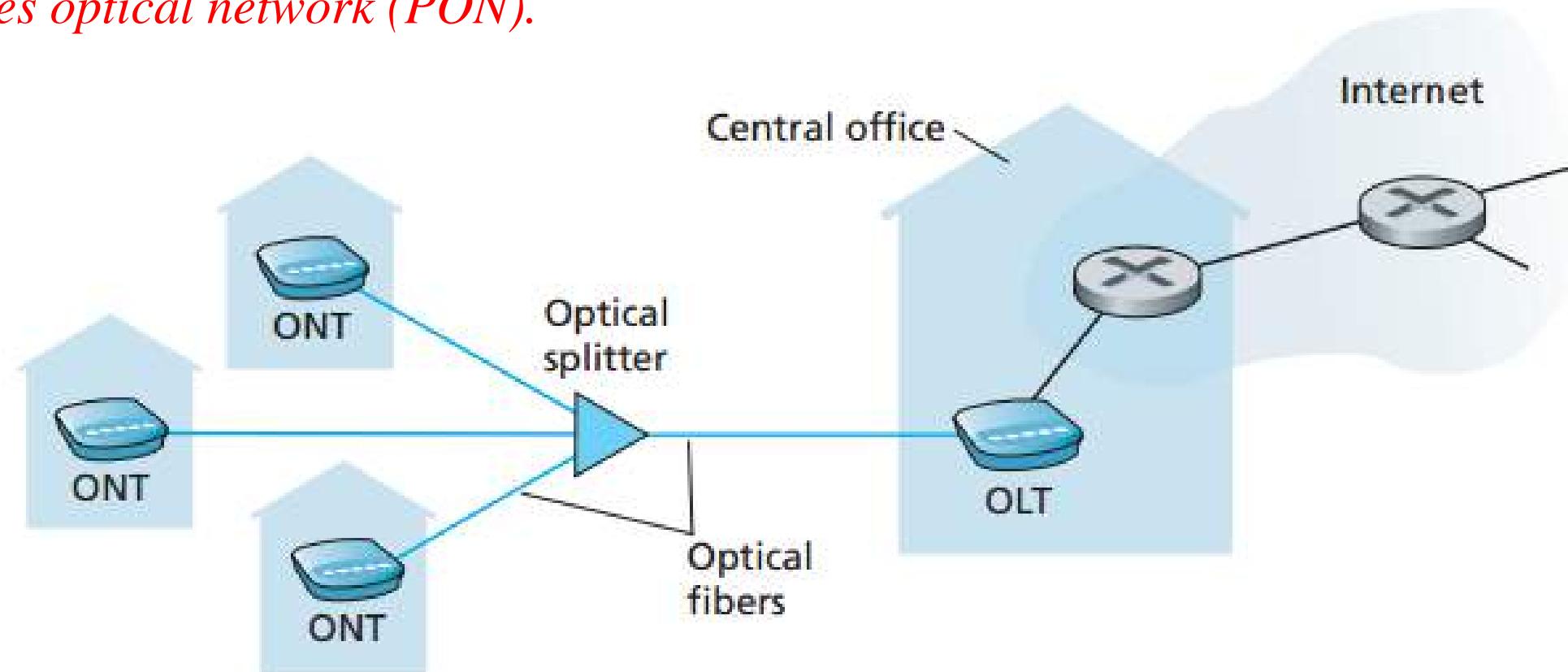
- *The fiber optics connect the cable head end to the neighbourhood level junctions, from which the traditional co-axial cable is then used to reach individual homes and apartments. Each neighbourhood junction typically supports 500 to 5000 homes.*
- *As both fiber optics and co-axial cables are involved it is often referred to as Hybrid Fiber Coax.*



- At the cable head end, the CMT (Cable Modem Terminator Systems) serves a similar function as DSLM in the DSL networks-such as turning the analog signal sent from several cable modems in many downstream home back into digital format.

Fiber to The Home (FTTH)

- It provides an dedicated optical fiber path from the central office (CO) directly to home.
- There are two types of Optical distribution network: Active optical network (AON) and Passives optical network (PON).



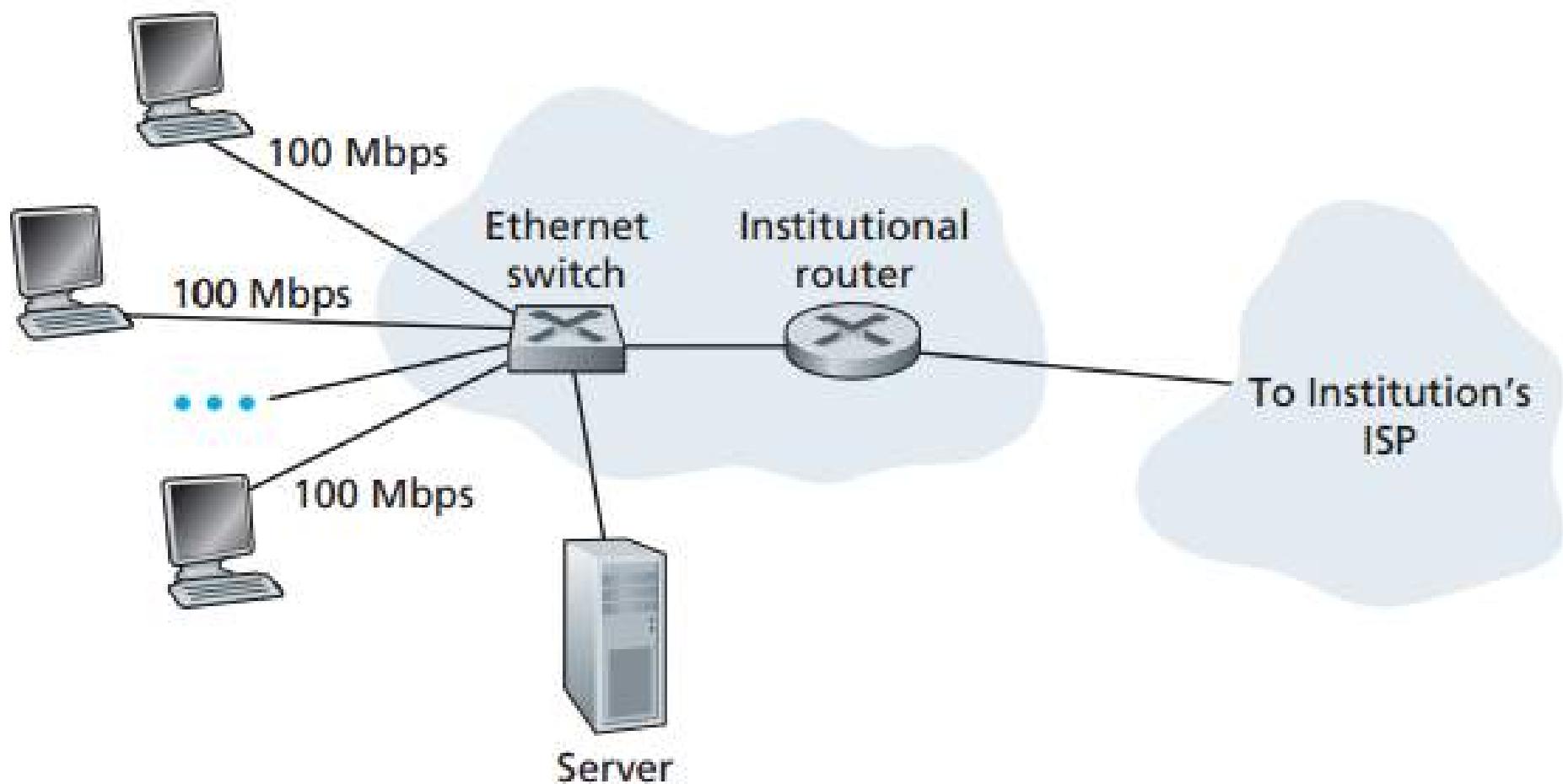
- The analog signal from many such houses are translated back into digital format at the DSLAM.

Fiber to The Home (FTTH)

- *Each home has an ONT (optical network terminator , which is connected to a optical splitter via a dedicated optical fiber link.*
- *The splitter combine a number of home (typically less then 100). The OLT (optical line terminator) provides the conversion between optical and electrical signals, connects to the internet via telco router*
- *FTTH can provide internet access rates in the Gbps range.*

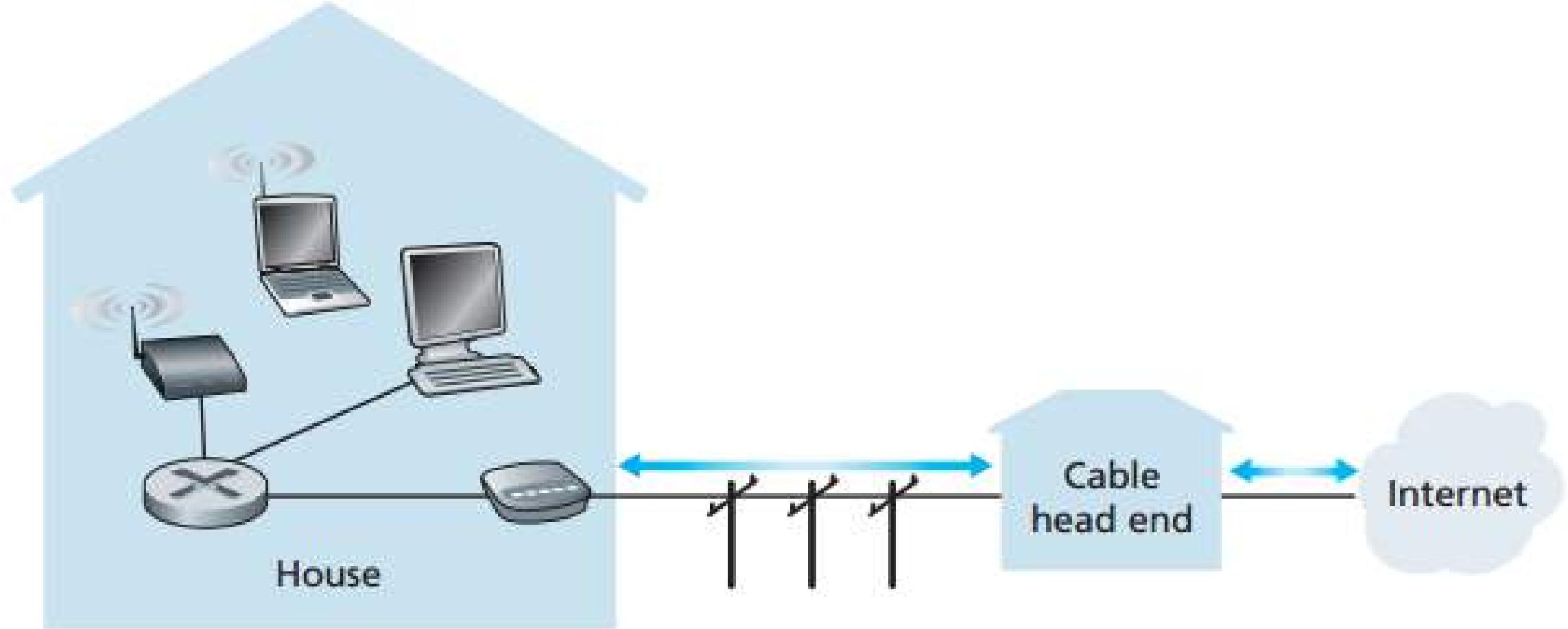
Access in Enterprise (and home): Ethernet and WiFi

- It is typically used in university campus, companies and home settings where many devices and IoT related applications are connected.
- *Ethernet users use twisted pair copper wire to connect to an Ethernet switch.*



Access in Enterprise (and home): Ethernet and WiFi

- *The Ethernet switch, or network of such interconnected Ethernet switches are then in turn connected to the larger internet.*
- *With Ethernet switch the user have 100 Mbps of data rate whereas the servers have 1 Gbps to 10 Gbps of data rate.*
- *The LAN (local area network) users must be in the range of 10 meters from the access point.*
- *Wireless LAN access based on IEEE 802.11 are mostly know as WiFi.*



A typical Home network

Wide- Area Wireless Access : 3G and LTE

- *Here the wireless devices (e.g. mobile phones) need to be within few kms from the base station to avail the 3G services and a data rate of typically 100 Mbps.*
- *Here the range is in kms whereas in WiFi the user need to be in tens of meter range from the access point ..*

Physical Medium

Guided Medium

- Twisted copper wire (Telephone lines)
- Coaxial cable (television cable wire)
- Fiber optic

Unguided Medium

- Terrestrial radio networks
 - Very short distance over two or three meters (keyboard , mouse, headset)
 - Local area networks for ten meters to a few hundred meters (wires LANs)
 - Wide area network for tens of kms (cellular access technology e.g. cell phone tower)
- Satellite radio channels

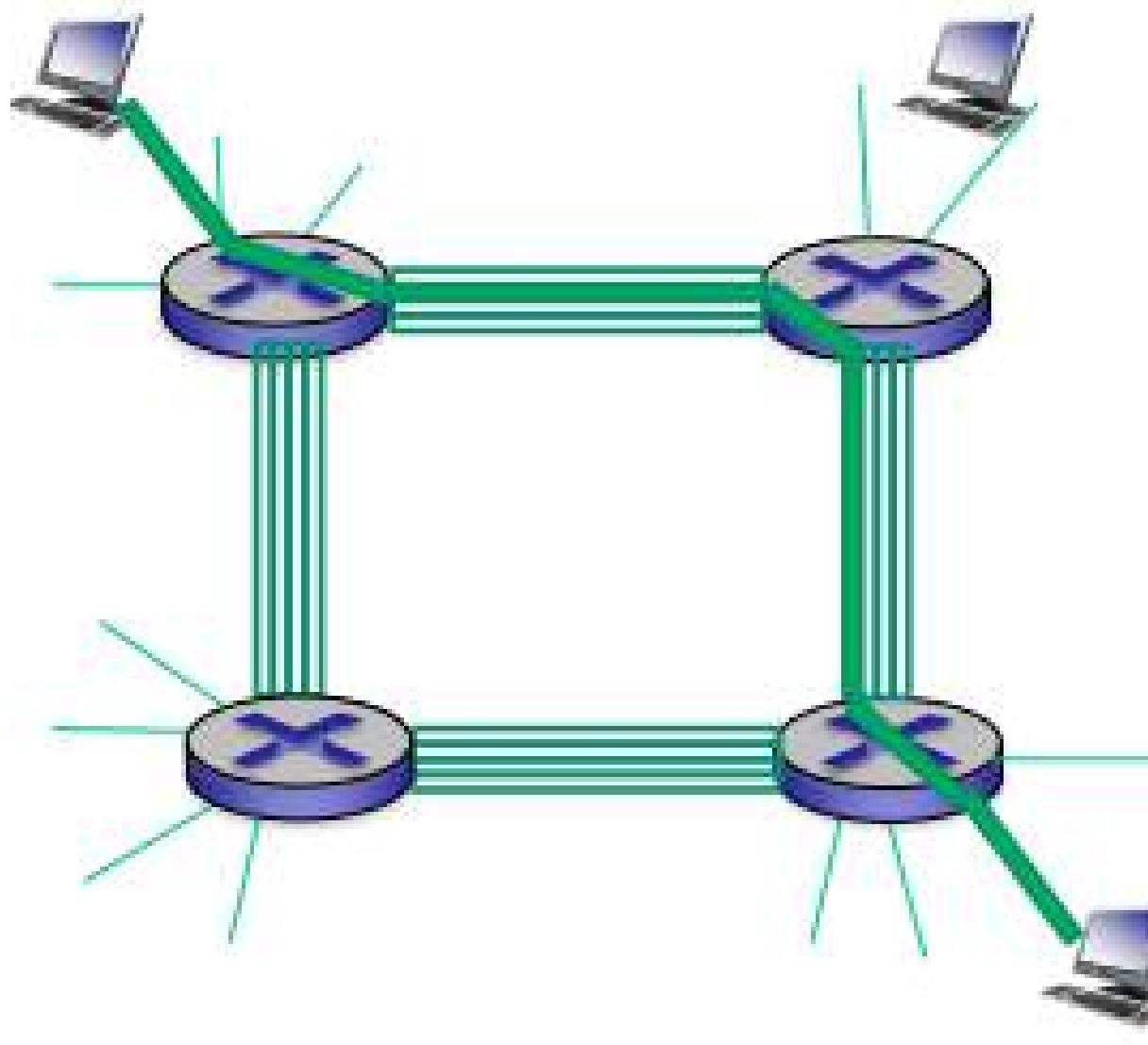
Circuit Switching

- ❑ A dedicated path is established between the sender and receiver.
- ❑ Before data transfer connection will be established first.
- ❑ The three phases of circuit switching are:
 - ❑ connection establishment
 - ❑ Data transfer
 - ❑ Connection termination

Packet Switching

- ❑ In packet switching, hosts breaks the messages into smaller packets.
- ❑ Forward packets from one router to the next, across links on the path from source to destination.
- ❑ Each packet is transmitted with full link capacity.
- ❑ Packet switching works with the principal of **Store-and –Forward**.
- ❑ **For sensing a packet of L bits over a link with transmission rate R bits/s, then the time required to transmit L bits is L/R secs.**

Circuit Switching



- ❑ A link consists of four circuits to support four connections.
- ❑ If each link between switches has a transmission rate of 1 Mbps, then each end-to-end circuit connection gets $\frac{1 \text{ Mbps}}{4} = 250 \text{ Kbps}$ of dedicated transmission rate.

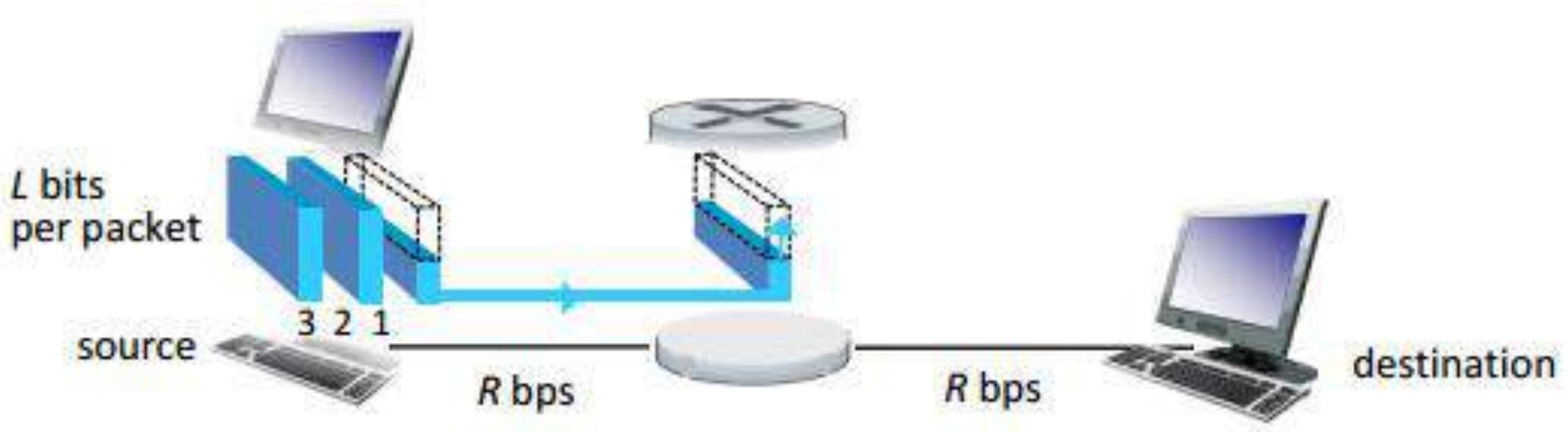
Module 1

Introduction to Computer Networks



Dr. Sunandita Debnath, IIIT Vadodara

Store-and-Forward



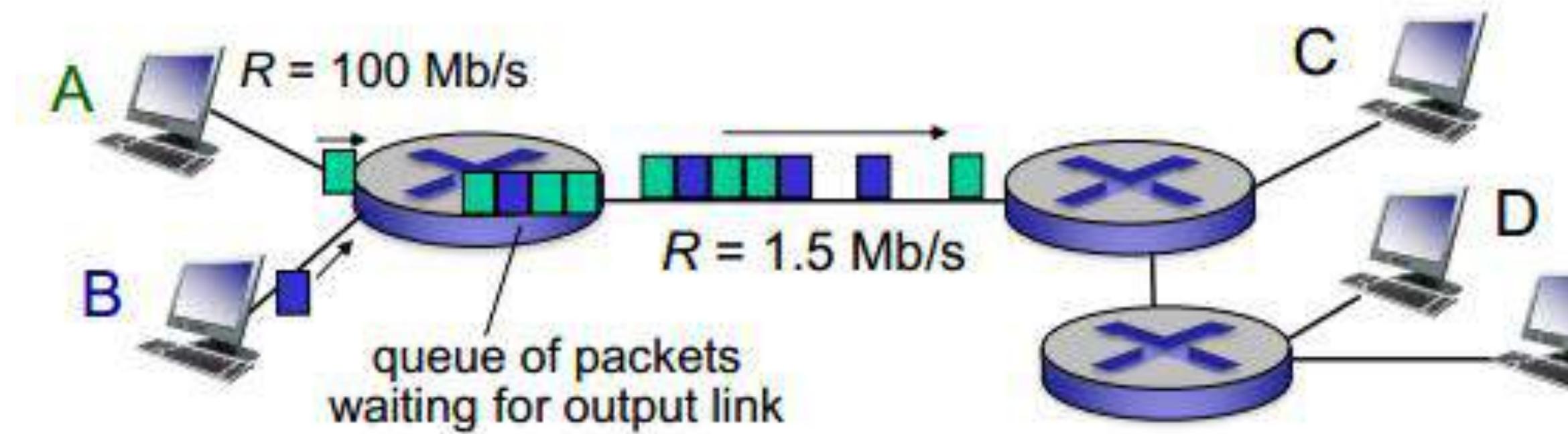
- The packet switch must receive the entire packet before it can *start* to transmit the first bit of the packet onto the outbound link. Instead it must *store* the packets' bits.
- Suppose the source is transmitting 3 packets of equal length of L bits and the link has a transmission rate of R bits/sec
- Until the entire bits of packet #1 will reaches at the router, the router will not begin transmission. So, the time required for the packet #1 to reach the destination is $(L/R+L/R)\text{secs}$ i.e. $2L/R$ secs.

Store-and-Forward

- Now for reaching all the *three* packets for reaching the destination is $(3L/R+L/R)$ secs.
- Here we have considered that the router has only one incoming and out going link.
- Now for sending one packet from source to destination over a path consists of N links (means $N-1$ routers have to crossed) each of transmission rate of R bits/sec.
- Then the total end to end delay is

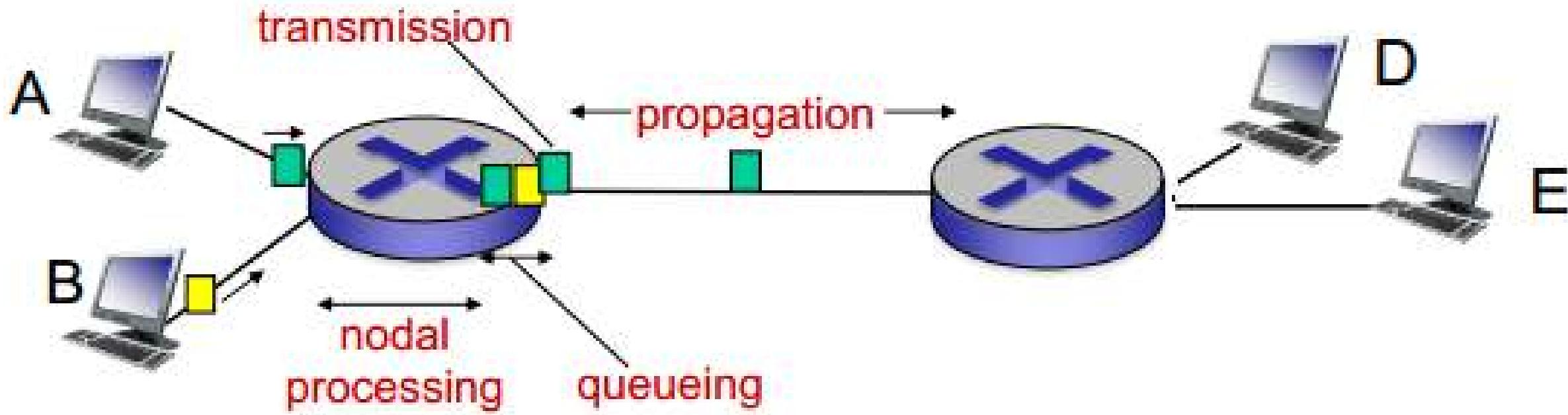
$$d_{end-to-end} = N \frac{L}{R}$$

Queuing delay and Packet loss



- For each attached link packet switch has an output buffer (also known as output queue) which stores packet which the router is about to send into that link.
- This queuing occurs when the arrival rate on the link exceeds the transmission rate of the link for a period of time.
- Two things happens in such situations:
- Packet will be queued, wait to be transmitted on the link
- Packets can be dropped (lost) if memory (buffer) fills

Four source of Packet delay



- A packet starts in a host (the source e.g. A or B), passes through a series of routers, ends its journey in another host (destination e.g. C or D). As packet travels from a node (host or router) to the subsequent node (host or router) along this path, suffers from several types of delay.

$$d_{\text{nodal}} = d_{\text{proc}} + d_{\text{queue}} + d_{\text{trans}} + d_{\text{prop}}$$

Processing Delay (d_{proc}) Processing delay in high speed routers are typically on the order of microseconds or less.

Queueing Delay (d_{queue}) packets will be transmitted in a first-come-first-served manner. waiting Time at the output link for transmission depends on congestion level of routers.

Transmission Delay (d_{trans}) If the length f packet is L bits and the transmission rate of the link from router A to B is R bits/sec then the transmission delay is

$$d_{trans} = \frac{L}{R} \text{ sec}$$

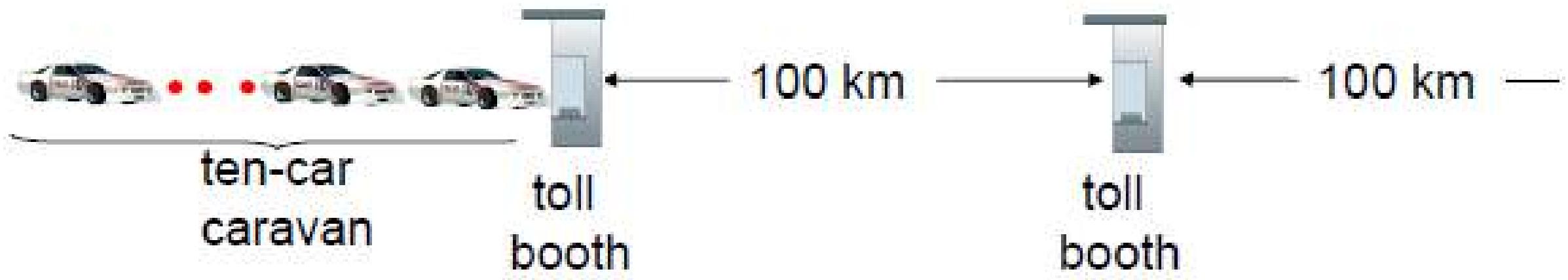
It is the amount of delay or time required to push all the bits of a packet into the link.
It is order of milisecs or microsecs.

Propagation Delay (d_{prop})

The propagation delay is given by

$$d_{prop} = \frac{\text{Distance between the two router (physical Length)}}{\text{Propagation speed of the link}} = \frac{d}{s}$$

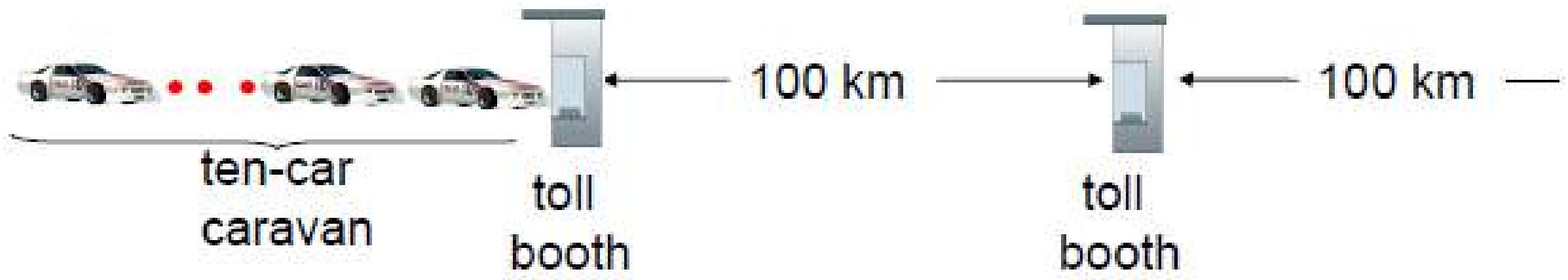
Caravan Analogy



- In a highway each of the tollbooths are 100 kms away.
- Suppose there are 10 cars travelling together as caravan, follow each other in a fixed order.
- Assume that the car travels on the highway at a rate of 100kms/hours.

$$d_{prop} = \frac{\text{Distance between the two router (physical Length)}}{\text{Propagation speed of the link}} = \frac{d}{s} = \frac{100 \text{ Kms}}{100 \text{ kms/hour}} \\ = 60 \text{ mins}$$

Caravan Analogy Contd...

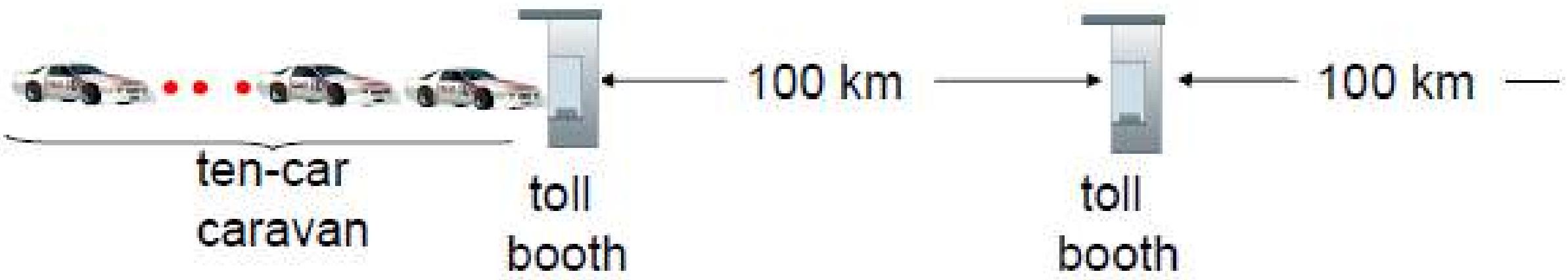


- Let the tollbooth services the one car at 12 secs. On the other way in 60 secs it will be able to service all the 10 cars.
- So the transmission delay of the caravan

$$d_{trans} = \frac{\text{Length of packet}}{\text{Transmission rate of the link}} = \frac{L}{R} = \frac{10 \text{ cars}}{5 \text{ cars/min}} = 2 \text{ mins}$$

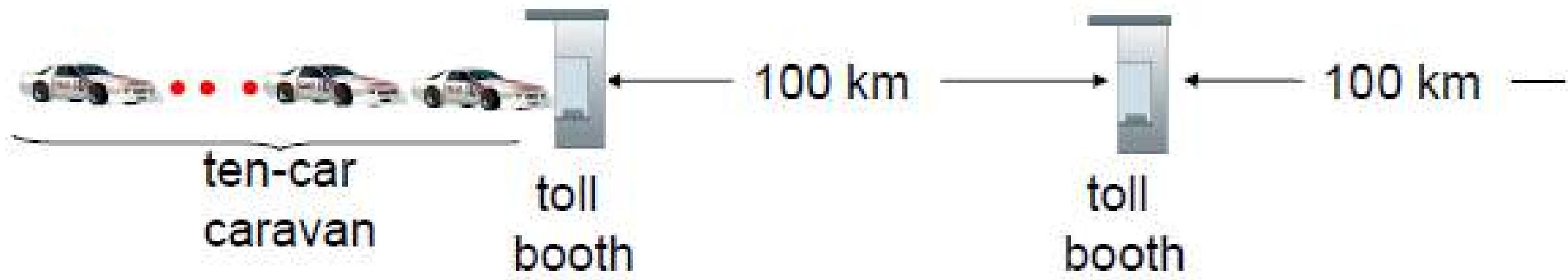
- Also assume that whenever the first car arrives at the tollbooth it waits at the entrance of the tollbooth until the other 9 cars arrives and lined up in sequence.

Caravan Analogy Contd...



- So finally the time from when the caravan is stored in front of a tollbooth until the caravan is stored in front of the next tollbooth is the sum of the
 $d_{trans} + d_{prop} = 60 + 2 = 62\text{mins}$

Caravan Analogy



- In a highway each of the tollbooths are 100 kms away.
- Suppose there are 10 cars travelling together as caravan, follow each other in a fixed order.
- Assume that the car travels on the highway at a rate of 1000kms/hours.

$$d_{prop} = \frac{\text{Distance between the two router (physical Length)}}{\text{Propagation speed of the link}} = \frac{d}{s} = \frac{100 \text{ Kms}}{1000 \text{ kms/hour}} = 6 \text{ mins}$$

Caravan Analogy Case2 Contd...

- Let the tollbooth services the one car at 1 mins secs.
- So the transmission delay of the caravan

$$d_{trans} = \frac{\text{Length of packet}}{\text{Transmission rate of the link}} = \frac{L}{R} = \frac{10 \text{ cars}}{1 \text{ cars/min}} = 10 \text{ mins}$$

- So the **transmission delay > propagation delay**. In this case the first car will reach the next tollbooth before the last care in the caravan leaves the first tollbooth.

Module 1

Introduction to Computer Networks



Dr. Sunandita Debnath, IIIT Vadodara

Queuing Delay and Packet Loss

Queuing Delay:

- Let a = average rate at which packet arrives at the queue a packets/sec
- R = transmission rate (in bits/sec) at which the bits are pushed out of the queue and loaded to the outbound link of the router.
- Assume each of the packet consists of L bits. So, the total size of traffic in bits La .

Traffic Intensity = $\frac{La}{R}$ (the desired traffic intensity should not be greater than 1)

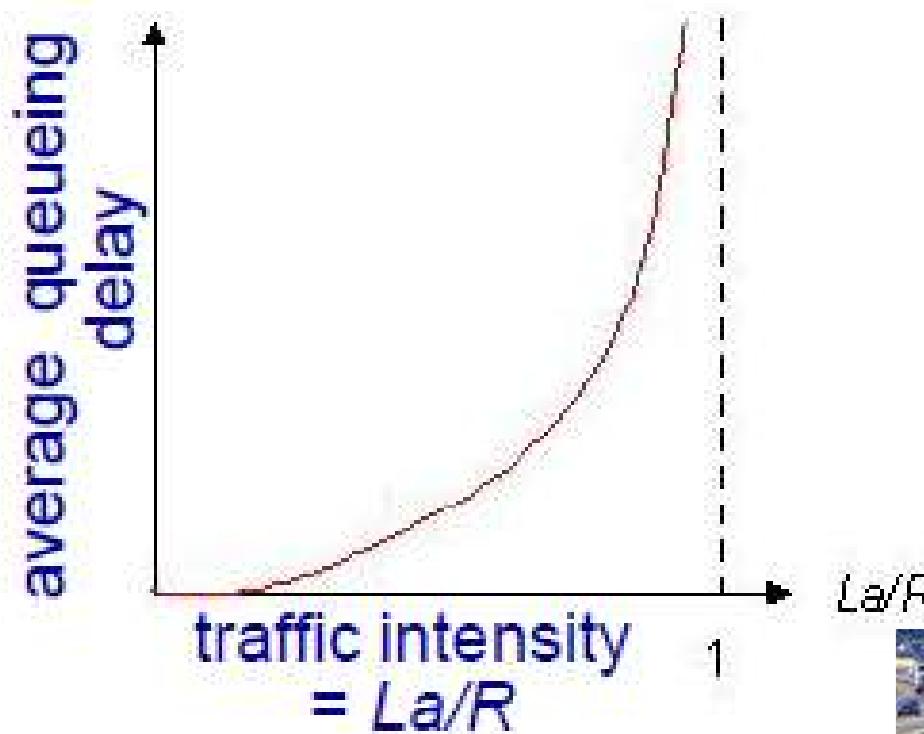
- If $\frac{La}{R} > 1$, the arrival rate is greater than transmission rate.
- If $\frac{La}{R} < 1$, the arrival rate is lesser than transmission rate.
- If packets arrive in bursts but periodically, there can be a significant average queuing delay. For example, suppose N packets arrive simultaneously every $(L/R)N$ seconds. Then the first packet transmitted has no queuing delay; the second packet transmitted has a queuing delay of L/R seconds; and more generally, the N th packet transmitted has a queuing delay of $(N-1)L/R$ seconds.

Queuing Delay and Packet Loss

Queuing Delay



$La/R \sim 0$

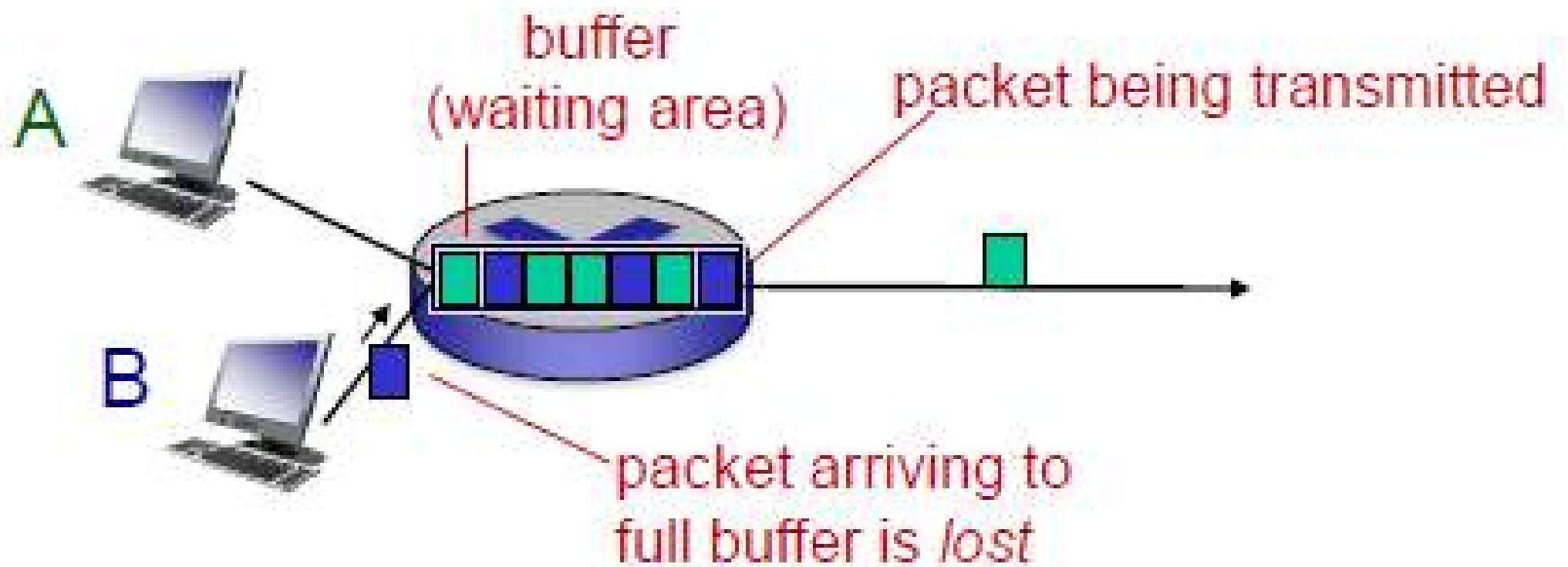


$La/R > 1$

Queuing Delay and Packet Loss

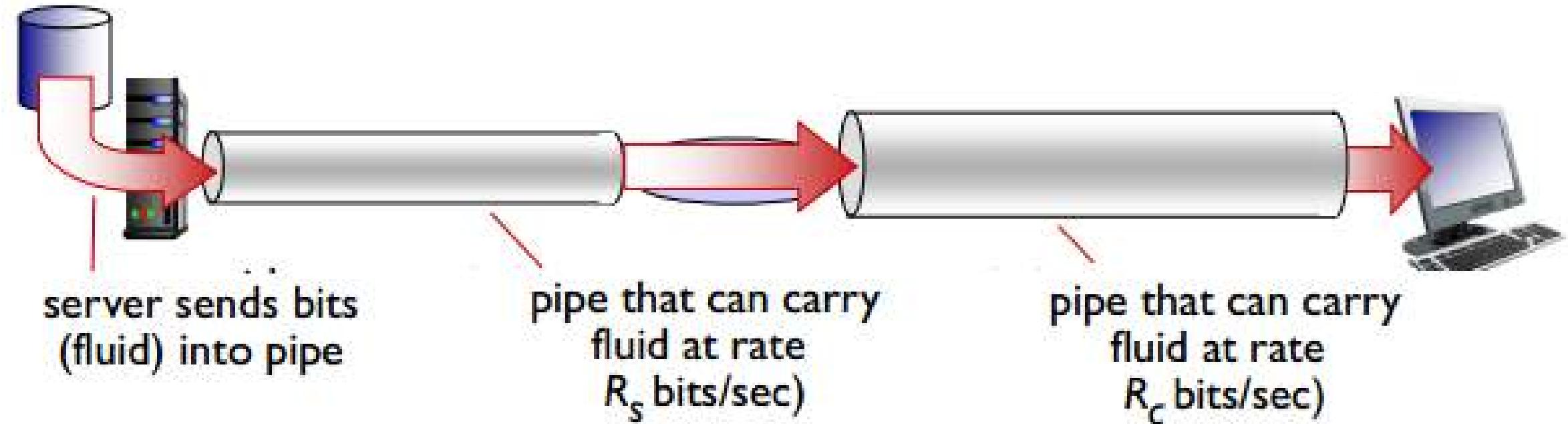
Packet Loss:

- Queue (buffer) has finite capacity
- If the queue is full, then any new packet arriving at the router will be lost or dropped.
- Lost packet may be retransmitted
- The fraction of lost packet increasing as the traffic intensity increases.



Throughput

- *The rate (bits/sec) at which bits transferred from sender to receiver.*
- *suppose the rate of the link between server and router is R_s bits/sec, and the rate of the link between the router and the client is R_c bits/sec.*
- *Two cases and occur $R_s < R_c$ and $R_s > R_c$*



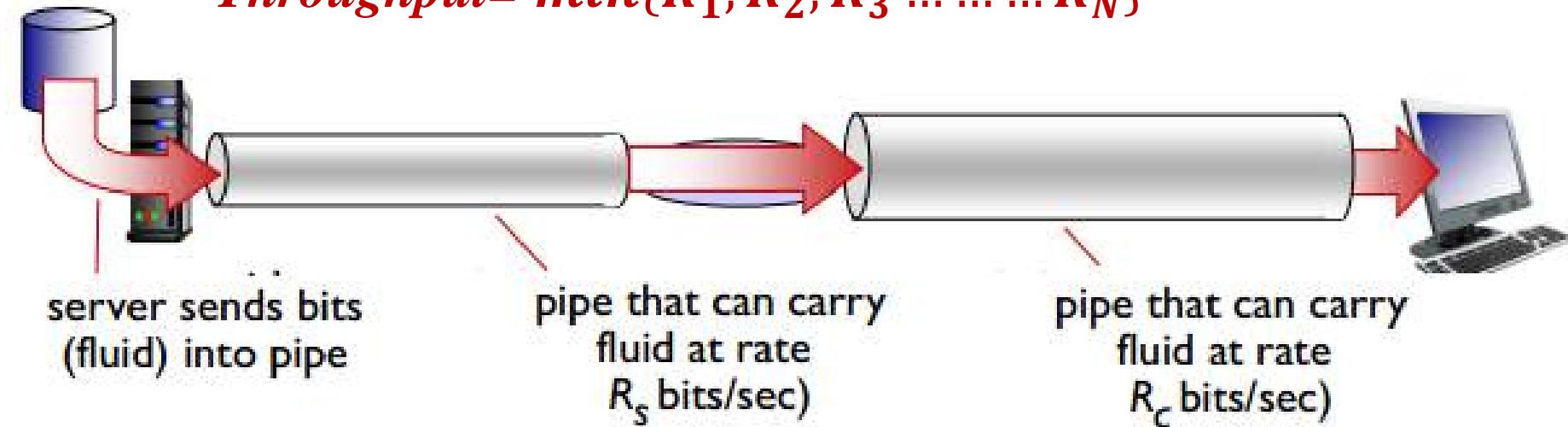
Throughput contd..

- $R_s < R_c$: the bits pumped by the server will flow right through the router and arrive at the client at a rate of R_s bits/sec, giving a throughput of R_s bps.
- $R_s > R_c$: the router will not be able to forward bits as quickly as it receives them from the server. In this case bits will only leave the router at a rate of R_c bits/sec, giving a throughput of R_c bps.
- Because of this condition the backlog of bits at the router waiting for transmission to the client will grow and grow –which is a most undesirable condition

$$\text{Throughput} = \min\{R_s, R_c\}$$

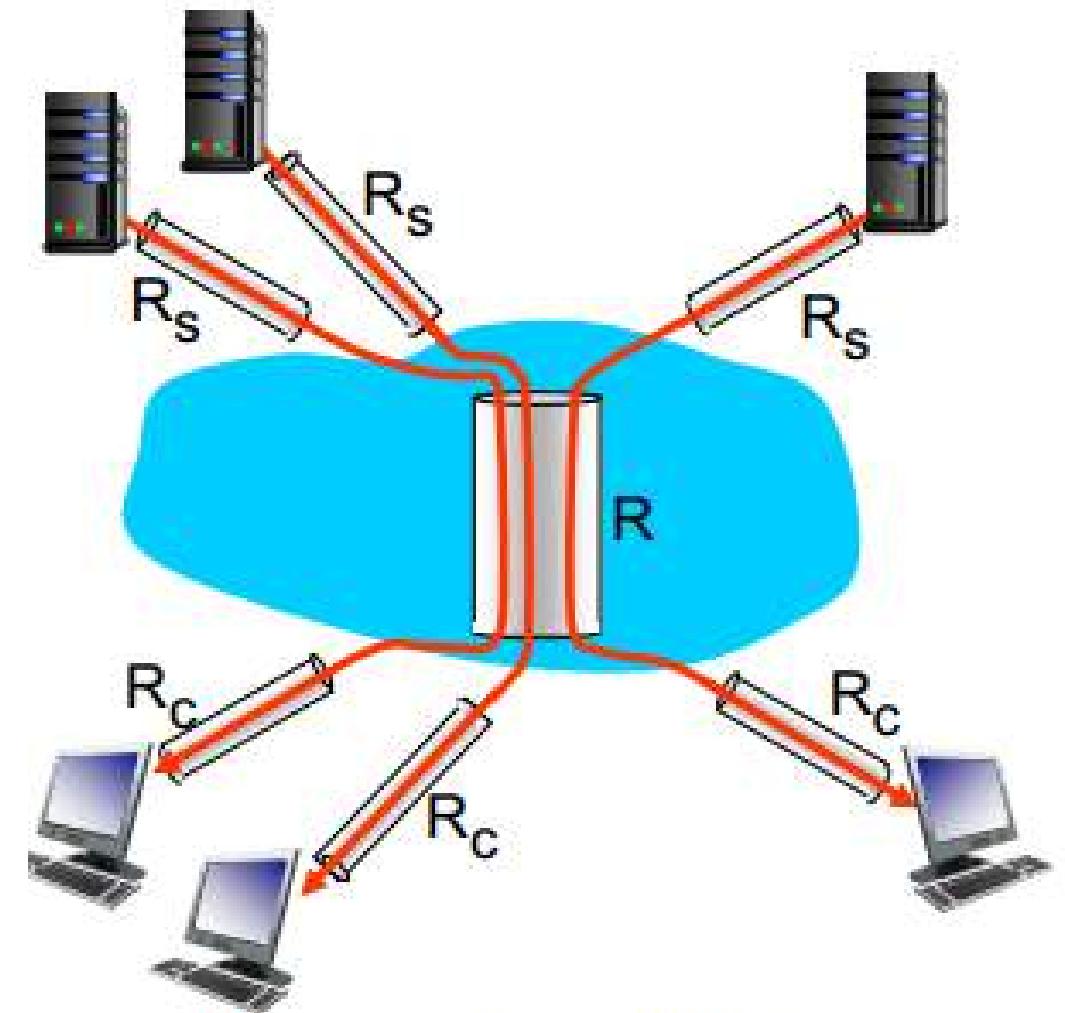
If there are N no. of links and transmission rates of R_1, \dots, R_N , then the throughput will be

$$\text{Throughput} = \min\{R_1, R_2, R_3, \dots, R_N\}$$



Throughput contd..

- Suppose there are 10 downloads from the server to client and these are the only traffic in the network.
- All server access link have a rate of R_s , and all client access links have a rate of R_c bps.
- The common link has a transmission rate of R bps.
- Suppose $R_s = 2 \text{ Mbps}$, $R_c = 1 \text{ Mbps}$ and $R = 5 \text{ Mbps}$. The R will be equally shared among the 10 links $5\text{Mbps}/10 = 500 \text{ Kbps}$.
Throughput= 500 Kbps.



10 connections (fairly) share backbone bottleneck link R bits/sec

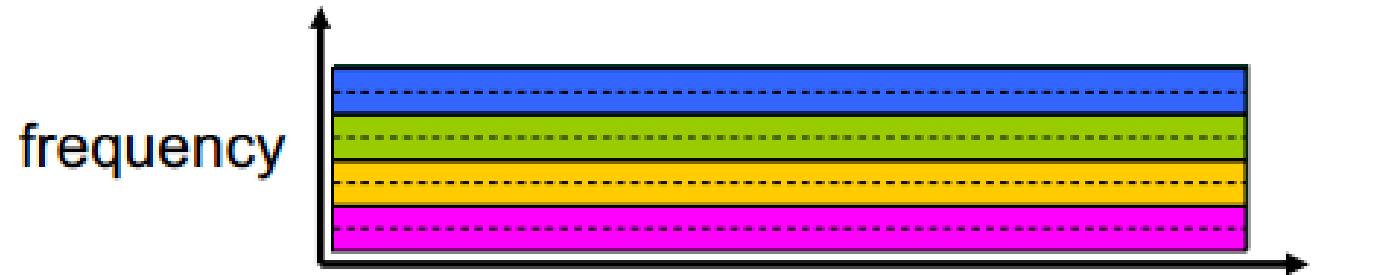
Note: Packet switches can be both routers and link layer switches.

Circuit Switching

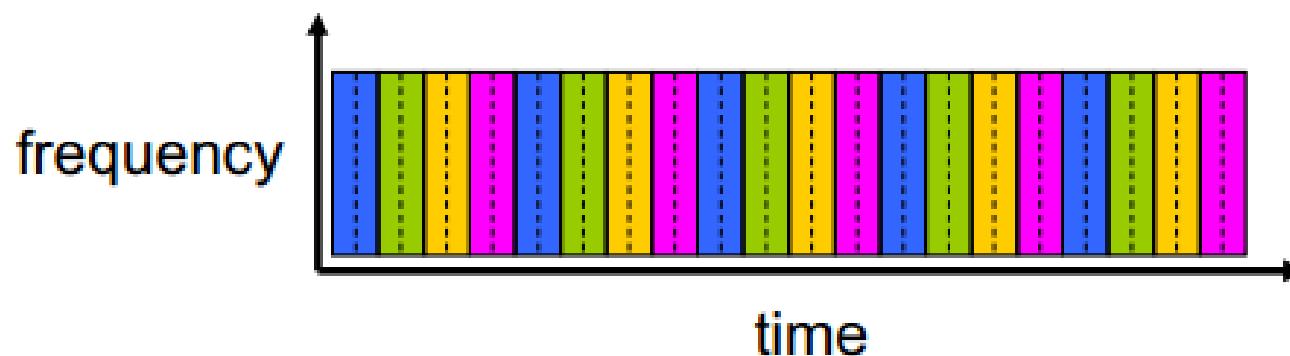
- TDM (Time Division Multiplexing)
- FDM (Frequency Division Multiplexing)

Example:

FDM

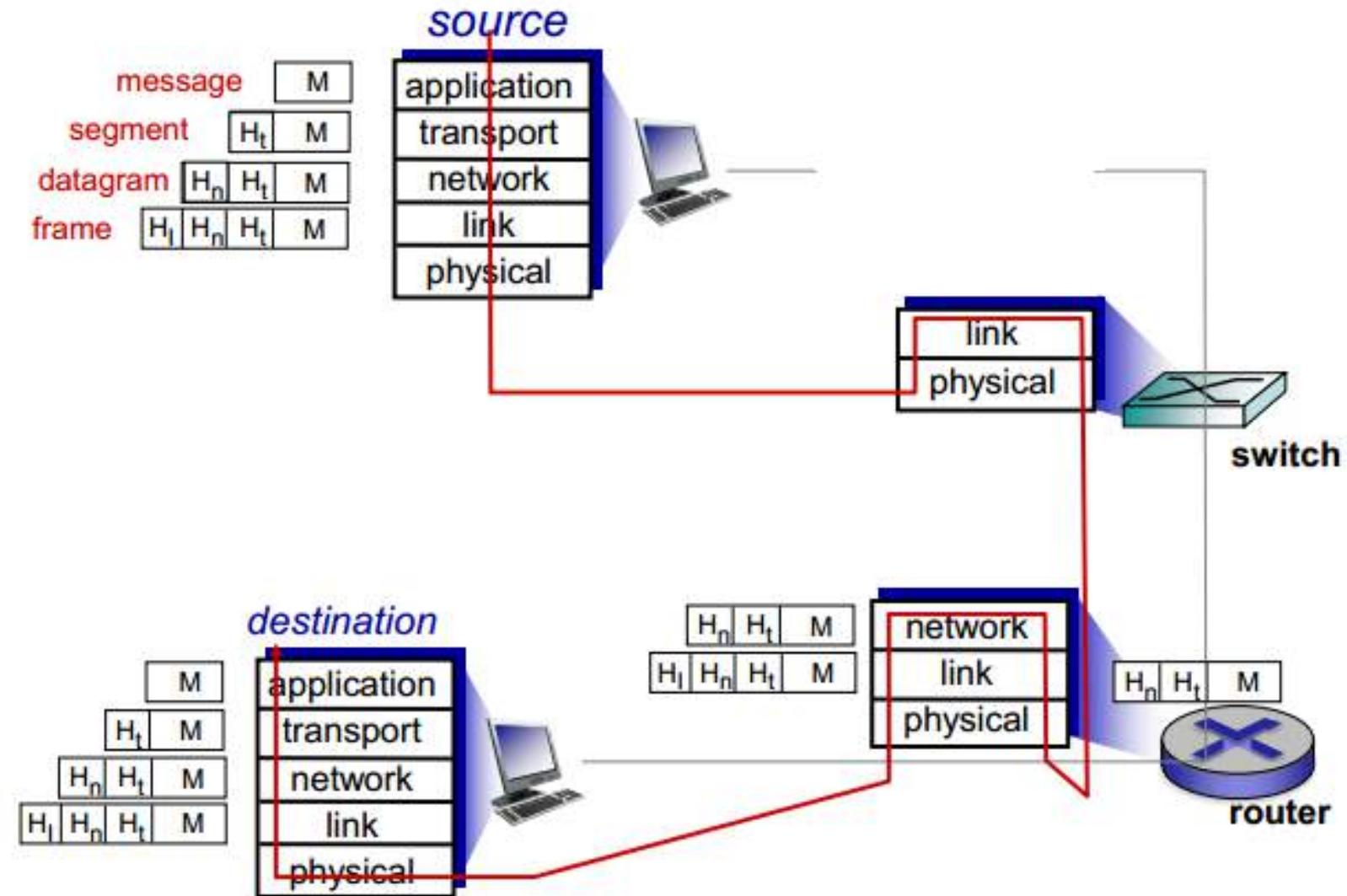


TDM



Encapsulation

- At each layer the a packet has two fields one is header fields and one is payload field.
- Payload is the typically a packet received from the above layer.



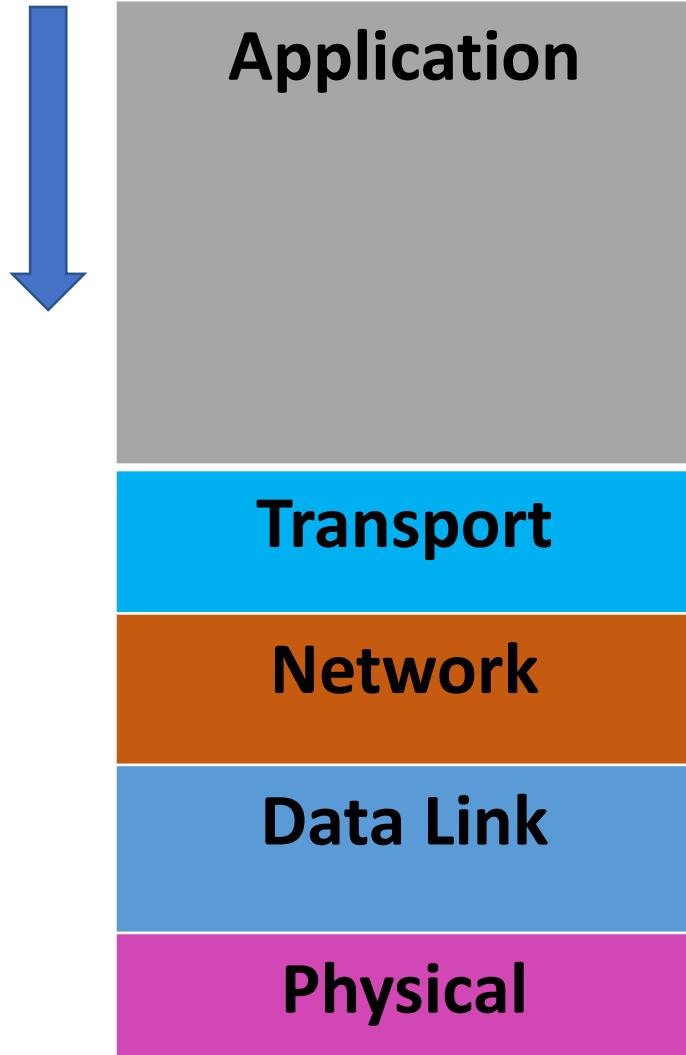
Module 1

Introduction to Computer Networks

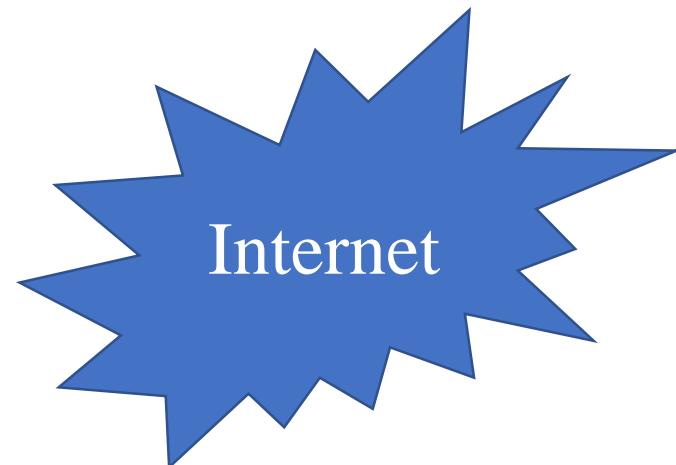
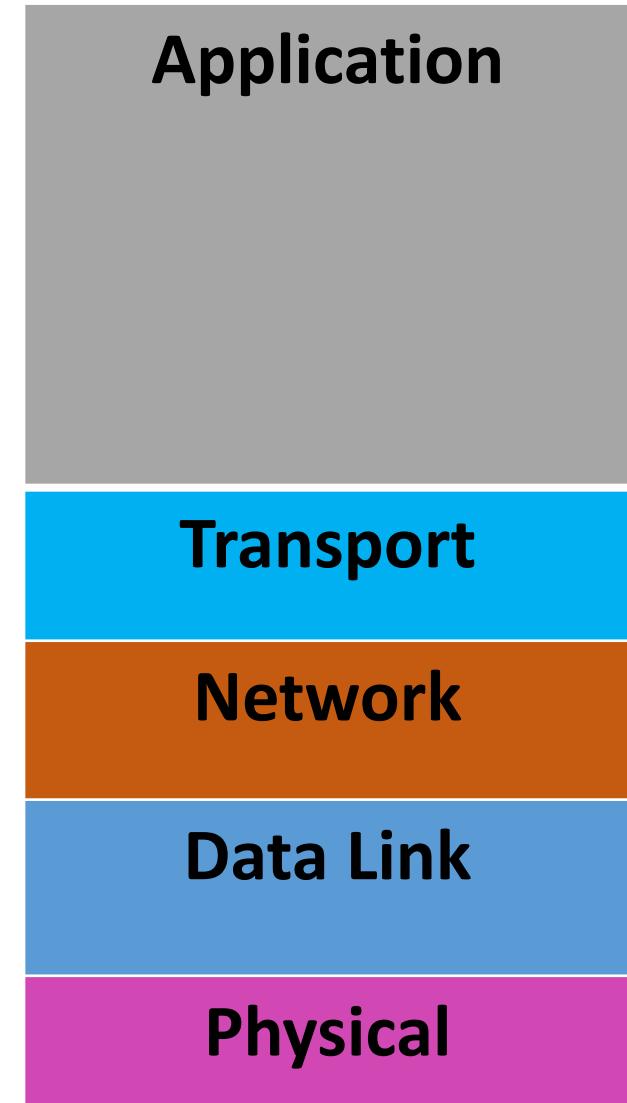


Dr. Sunandita Debnath, IIIT Vadodara

Sender



Receiver



Data Link Layer

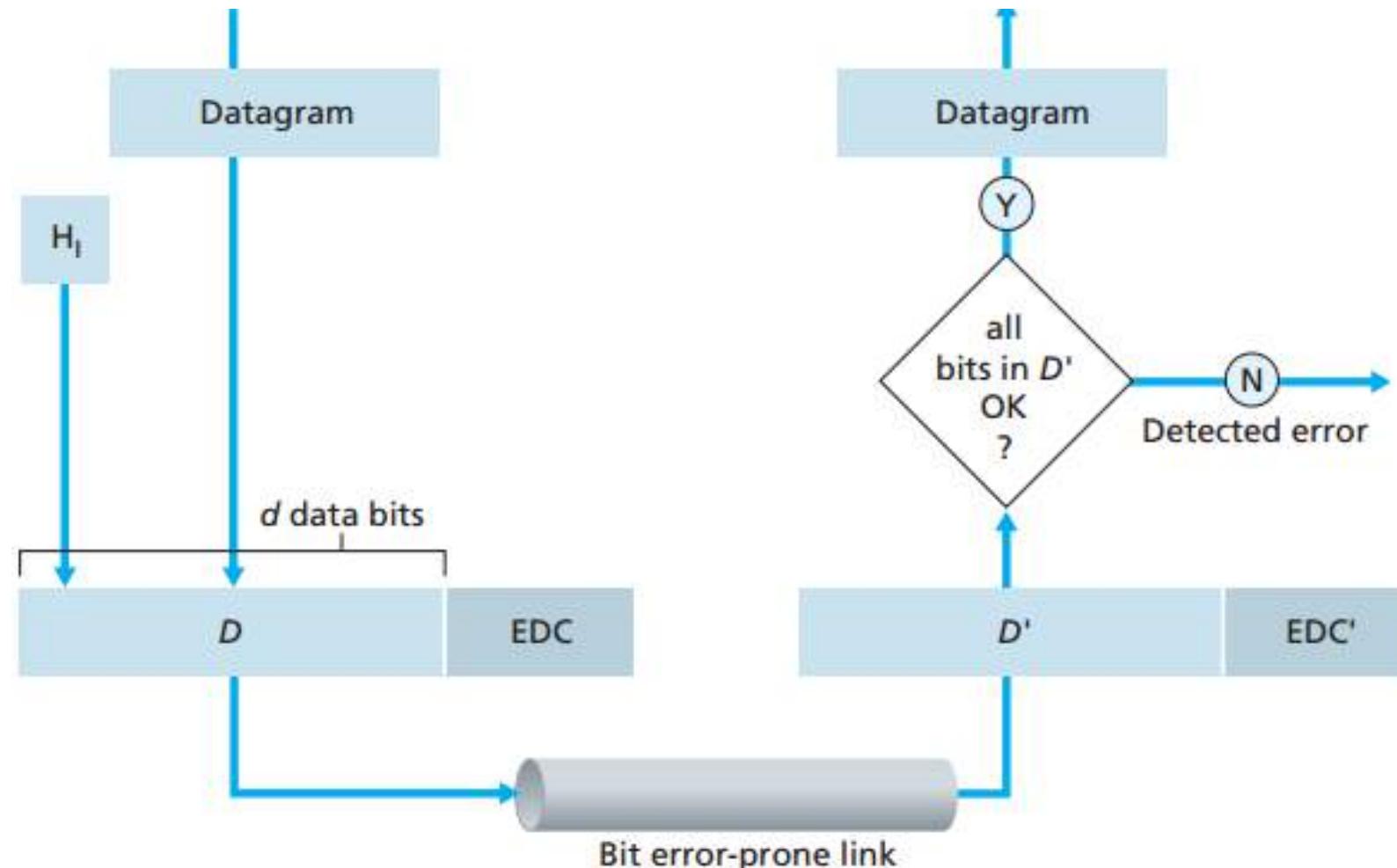
- Data link layer is also known as Layer 2. Data link resides between the network layer and physical layer.
- Datalink layer are responsible for transferring datagram from one node to physically adjacent node over a link.
- **Switch is a layer 2 device.**

Functions of Data Link Layer

- **Framing:** *encapsulate datagram into frame, i.e. adding header and trailer.*
- **Link access:** *Channel access if share media. A MAC protocol specifies the rules by which a frame is transmitted onto the link.*
 - *When there is a point-to-point connection between a sender ad receiver i.e. a single sender at one end of the link and a single receiver at another end of the link, then the MAC protocol is simple means whenever the link is idle the sender can send.*
 - *When multiple nodes share a single broadcast link-the multiple access problem occurs and the MAC protocol has to coordinate the frame transmissions of the many nodes.*
- **Reliable delivery:** **Reliable delivery services are offered by both transport layer and data link layer.**
 - *It is important for high error rate links such as wireless links, where the goal of correcting an error locally is more desirable than retransmission of the datagram.*
 - *Seldom used in low bit error links such as fiber and twisted pair wires.*

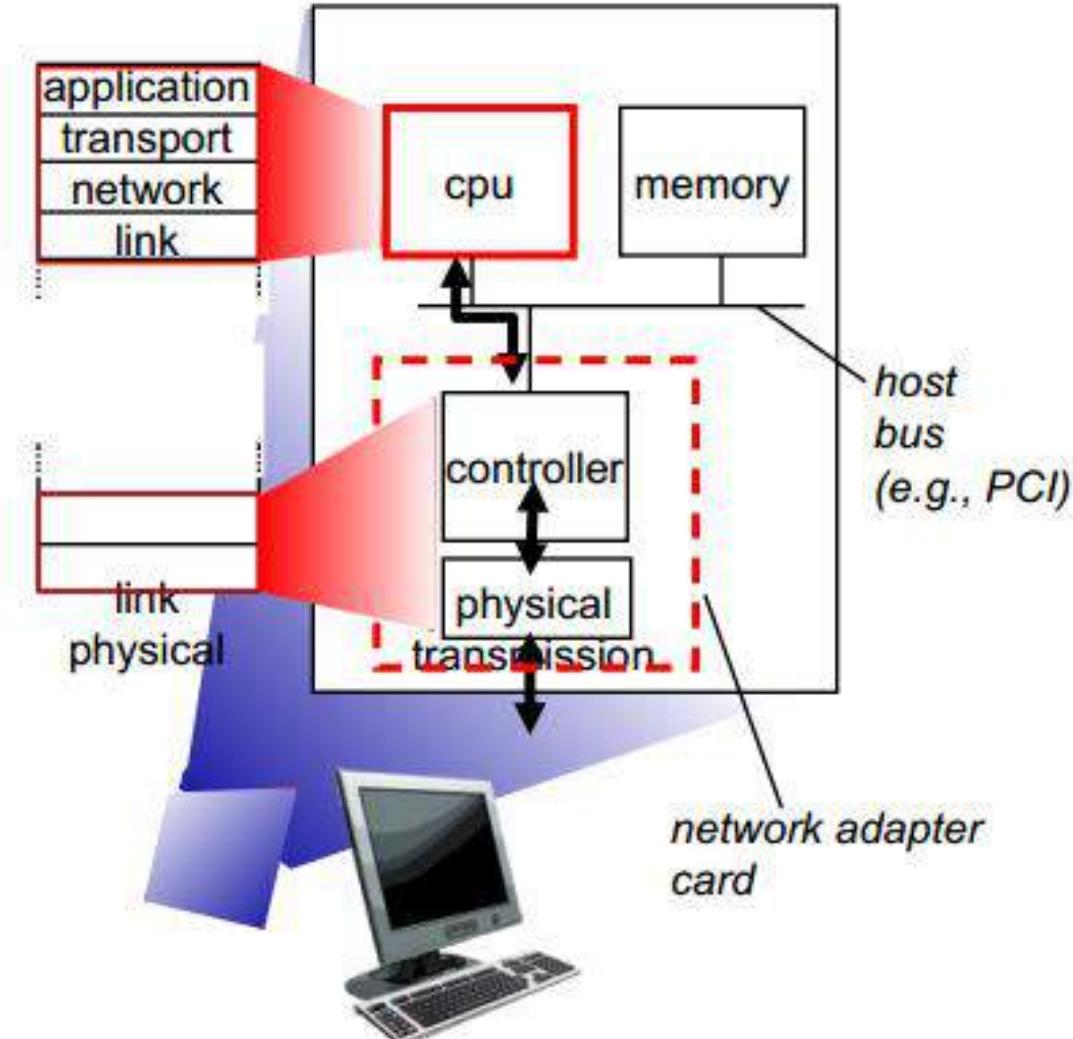
Functions of Data Link Layer Contd...

- **Error detection and Error correction:** *The transmitting node include error-detection bits in the frame, and having the receiving node perform an error check .*



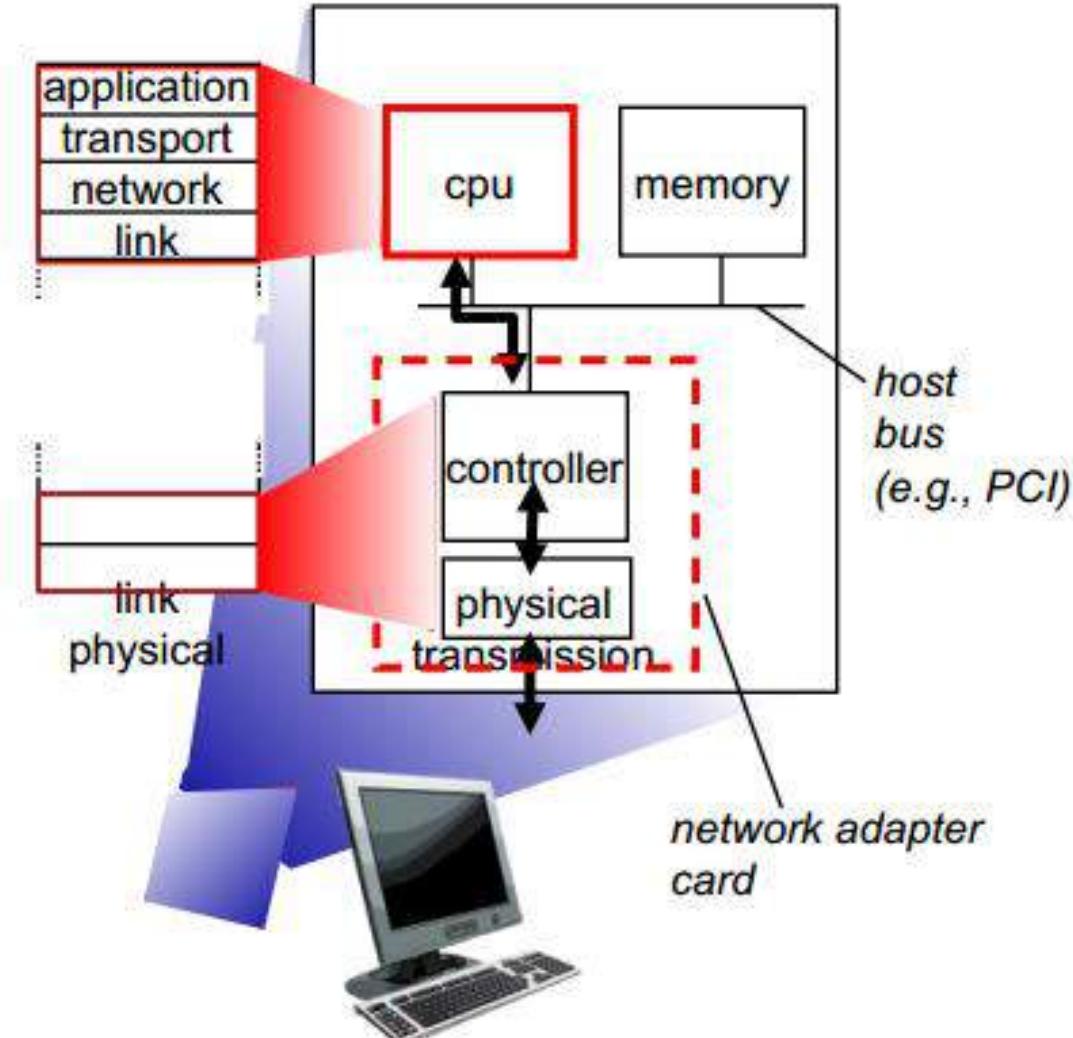
Where is this link layer implemented

- *Link layer is mostly implemented in the network adapter i.e. in the NIC (Network Interface Card) card*
- *At the heart of the network adapter is the link layer controller that implement many of the link layer services such as framing, link access, error detection and so on.*
- *Now a days network adapters are being integrated onto the hosts motherboard (LAN on motherboard configuration).*



Where is this link layer implemented contd..

- On the sender side, the controller takes the datagram that has been created and stored in the host memory by the higher layers of protocol stack, encapsulate the datagram in a link layer frame and transmit the frame into the communication link, following the link access protocol.
- On the receiver side, a controller receives the entire frame and extracts the network layer datagram.
- If the link layer performs error detection, then the sending controller that sets the error-detection bits in the frame header and is the receiving controller that performs error detection.
- Link layer is a combination of hardware and software-the place where software meets hardware



Module 1

Introduction to Computer Networks



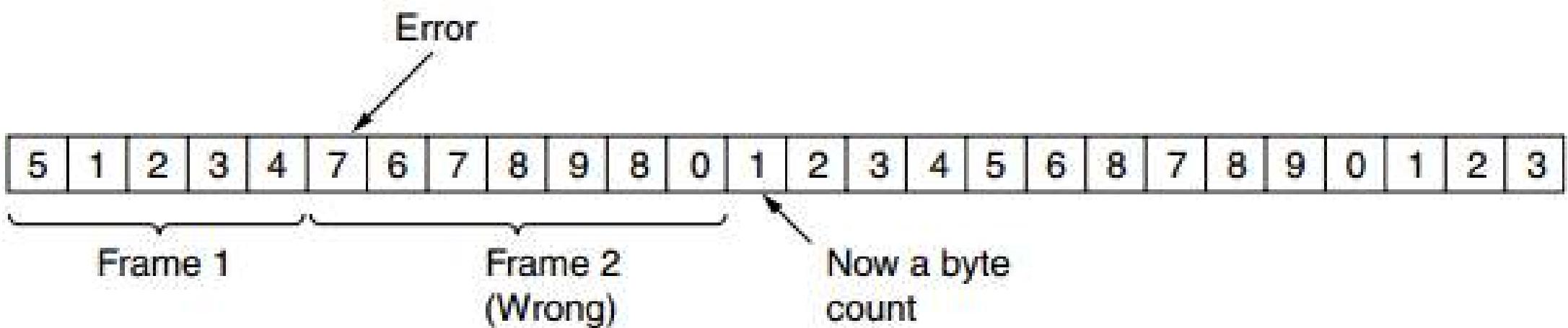
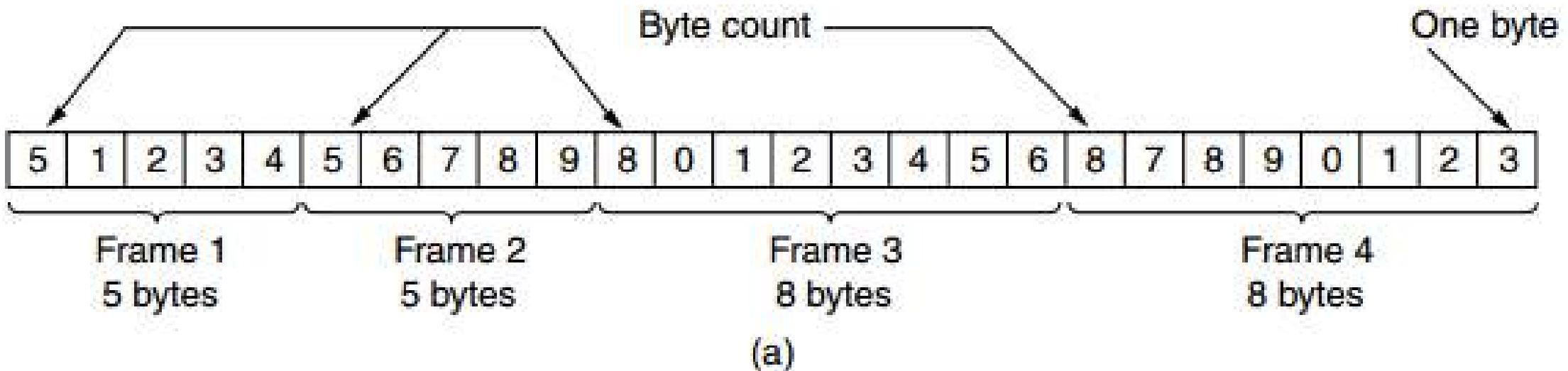
Dr. Sunandita Debnath, IIIT Vadodara

Framing

- Byte count
- Flag bytes with bytes stuffing
- Flag bits with bits stuffing
- Physical layer coding violation

Framing

➤ Byte count



Framing

➤ Flag Byte with Byte Stuffing



- Here the resynchronization problem in byte count is overcomed by inserted a special bytes at the starting and ending of a frame as delimiters, this special bytes are called Flag Byte
- Thus if the receiver ever loses synchronization then it will search for two consecutive Flag bytes to find the end of one frame and start of the next frame.

Framing

➤ Flag Byte with Byte Stuffing contd.



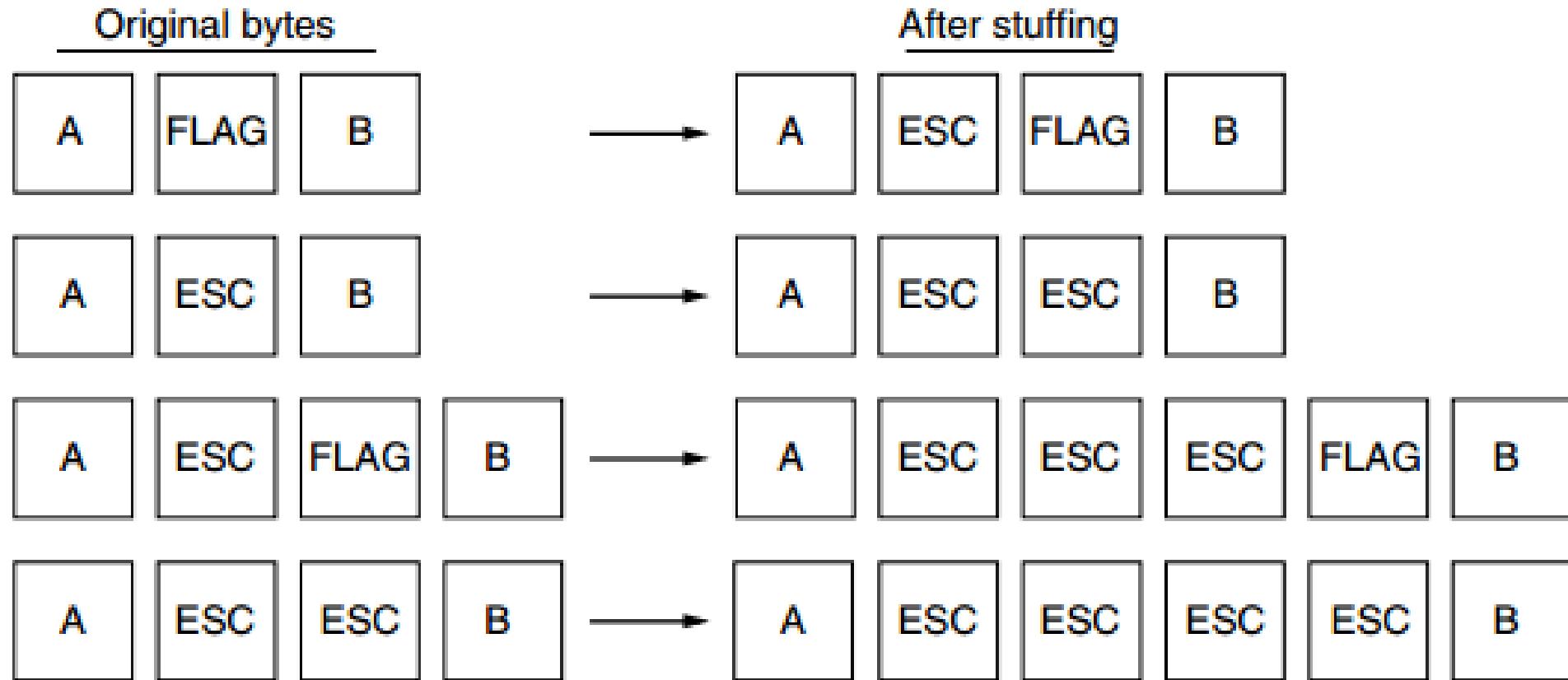
1100010011001100

- If the same sequence of '0' and '1' which indicates the Flag bytes occurs in the middle of the data.
- To solve this problem is to have the sender's data link layer insert a special escape byte (ESC) just before each "accidental" flag byte in the data.
- Thus, a framing flag byte can be distinguished from one in the data by the absence or presence of an escape byte before it.
- The data link layer on the receiving end removes the escape bytes before giving the data to the network layer. This technique is called byte stuffing.

Framing

Flag Byte with Byte Stuffing contd.

- Now if the data itself consists of an ESC byte then what is the solution.
- It is again stuffed with an escape byte. At the receiver, the first escape byte is removed, leaving the data byte that follows it.
- the byte sequence delivered after destuffing is exactly the same as the original byte sequence.



Framing

Flag Bit with Bit Stuffing

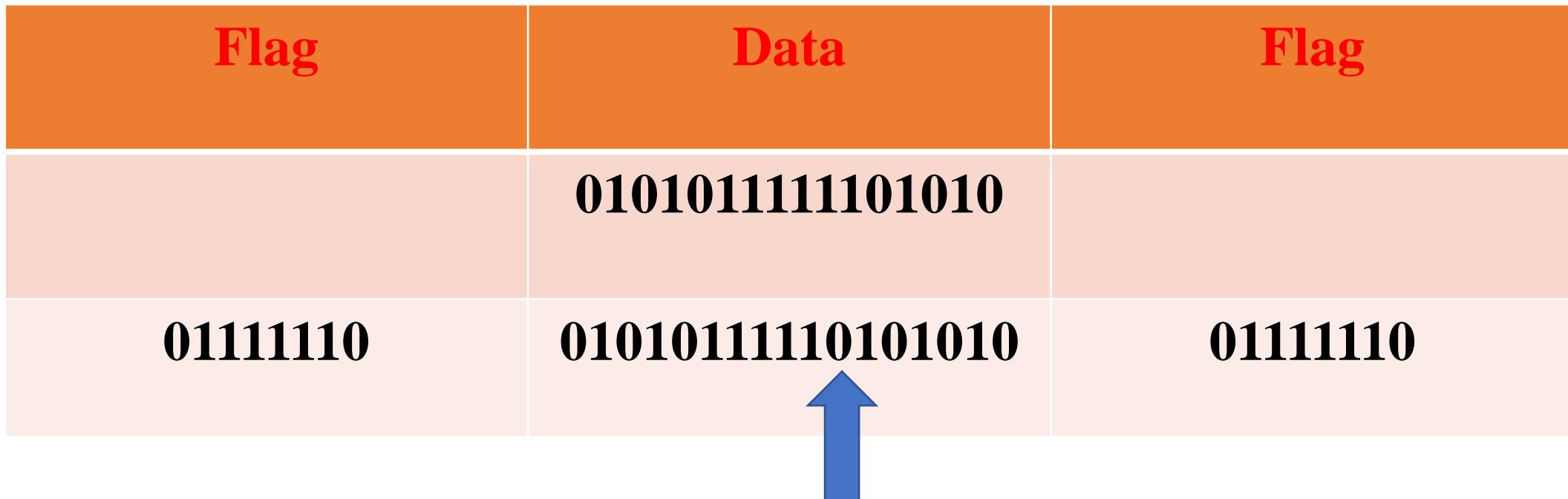
- *Byte stuffing has one disadvantage of that it is tied around to use of 8-bits byte.*
- *Frames can contain any arbitrary number of bits. It was for the protocol HDLC (High Level Data Link Control) protocol.*
- *Each of the frame begins and end with a special sequence of bits **01111110** or **0x7E** in Hex. This pattern is a Flag byte.*



Framing

Flag Bit with Bit Stuffing contd...

- If the sender data link layer finds the data consists of Flag byte then it automatically stuff one zero bit after five consecutive '1's.
- The receiver finds five consecutive 1 bits, followed by a 0 bit, it automatically unstuffs (i.e.) delete the 0 bit.



Framing

Physical layer coding Violations

- *In bit stuffing and byte stuffing the length the data increases unnecessarily.*
- *This takes helps of physical layer where there are some reserved signal which will be used to indicate the starting and ending of a frame.*

Module 1

Introduction to Computer Networks



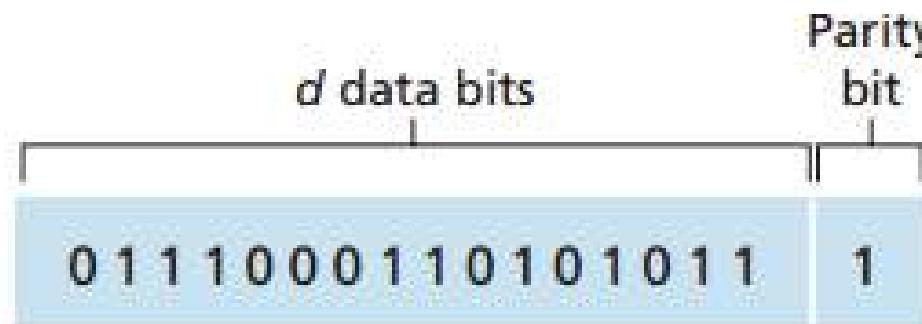
Dr. Sunandita Debnath, IIIT Vadodara

Error Detection and Correction Techniques

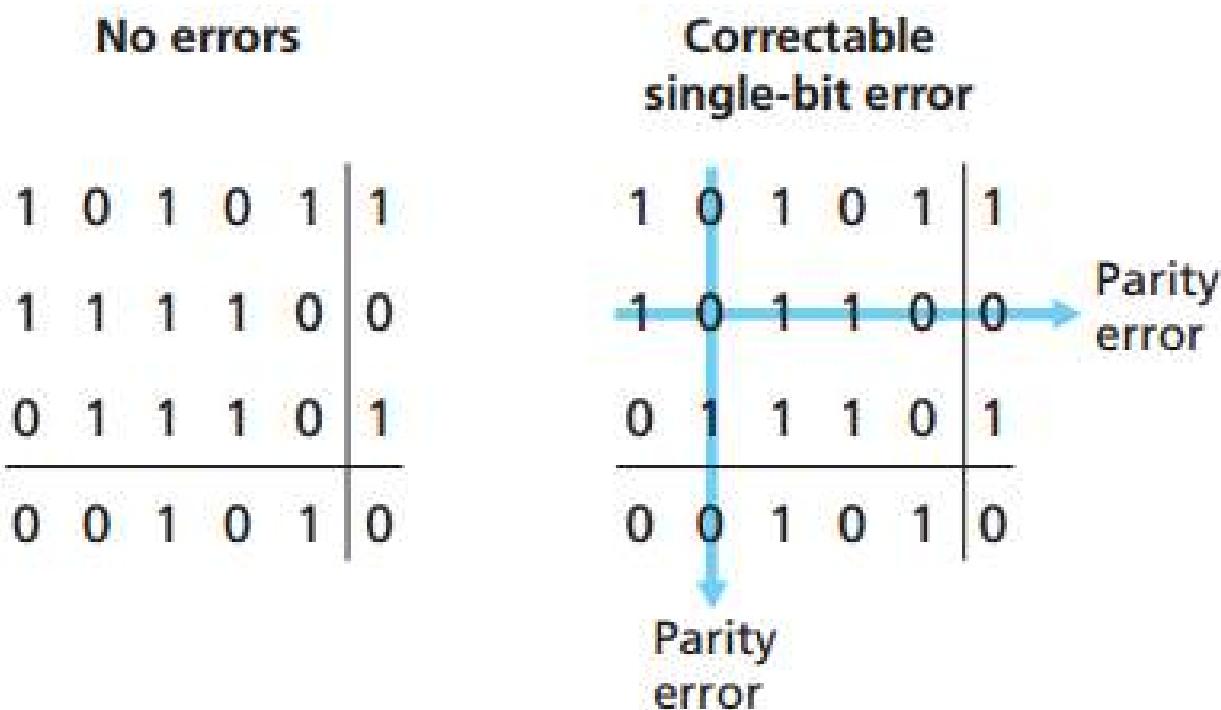
- *Parity Check*
- *Checksum*
- *Cyclic Redundancy Check (CRC)*

Error Detection and Correction Techniques

➤ Single Parity Check



➤ Two-dimensional Parity Check



Error Detection and Correction Techniques

Checksum(at the Sender side)

- Break the original message into ‘k’ number of blocks with ‘n’ bits in each block.
- Sum all the ‘k’ data blocks
- Add the carry to the sum if any.
- Do 1’s complement of the sum and this will be the checksum bit which will be appended with the transmitted data.

Checksum(at the Receiver side)

- Sum all the ‘k’ data blocks with the checksum bits
- If the resultant sum is all ‘1’s then the received data bit is correct and error free.

Error Detection and Correction Techniques

Cyclic Redundancy Check (CRC) at the Sender side

- *Find the length of the divisor 'L'.*
- *Append (L-1) bits to the original message*
- *Perform binary division operation*
- *Remainder of the divisor is the CRC*

Cyclic Redundancy Check (CRC) at the Receiver side

- *Divisor is common for both the transmitter and receiver.*
- *When there is no remainder or all 0 's at the remainder , the receiver can conclude that the transmitted bit was detected error free.*

Error Detection and Correction Techniques

CRC(at the Sender side)

Divisor 1001 (Length of Divisor L = 4)

Data 101110 (Append (L-1) zeros)

CRC bits 011

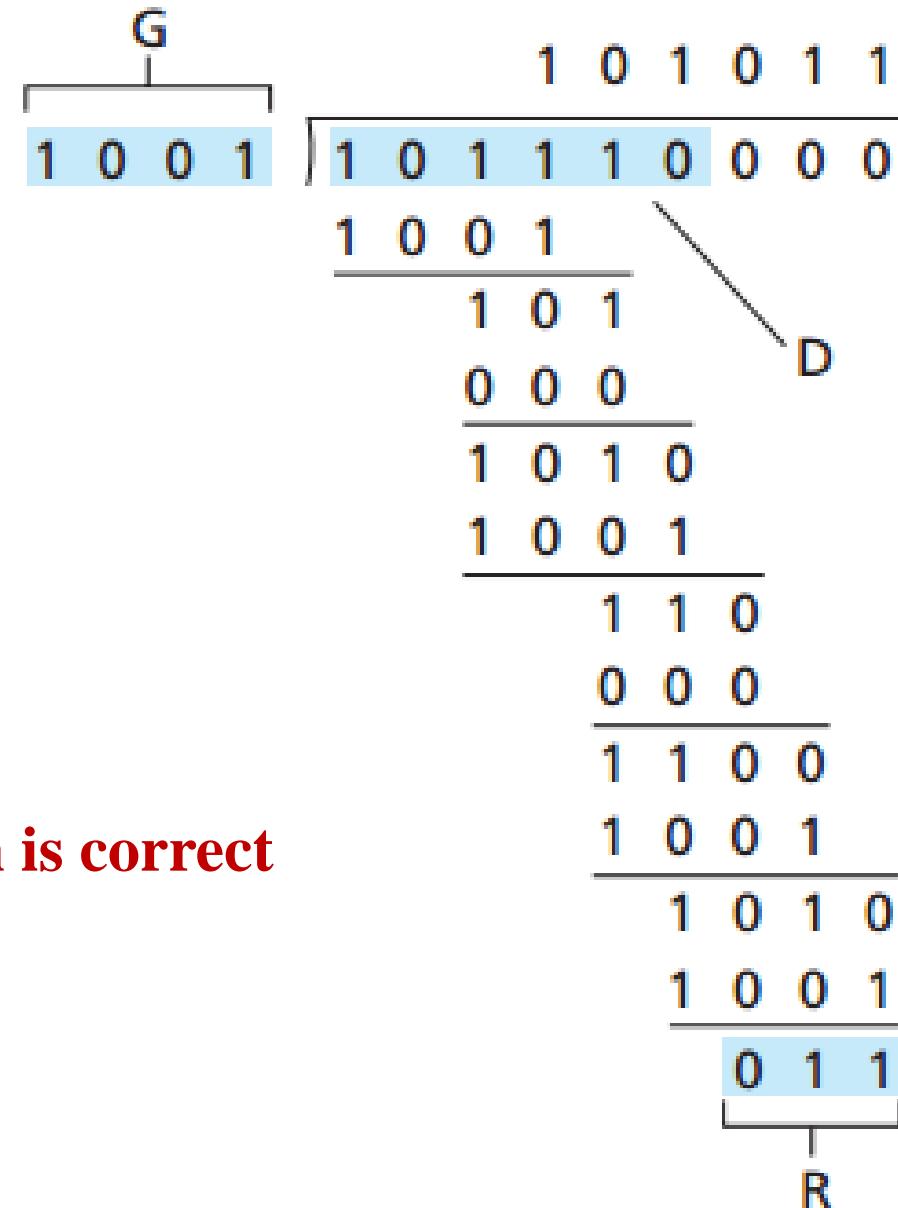
Transmitted data 101110011

CRC(at the Receiver side)

Divisor 1001 (Length of Divisor L = 4)

Received data 101110011

If no remainder (all '0's)is there than received datagram is correct



There are two types of network links in Data link layer

Point to Point link

It consists of a single sender at one end of the link and a single receiver at the other end of the link. Protocols for point-to-point link are

Point-to-point protocol (PPP)

High-level Data Link control (HDLC)



shared wire (e.g., cabled Ethernet)



shared RF (e.g., 802.11 WiFi)



shared RF (satellite)

Broadcast link

It can have multiple sending and receiving nodes all connected to the same single shared broadcast channel..

➤ *E.g. Ethernet and Wireless LANs*

In computer networks broadcast channels can both send and receive . The main problem in this scenario is that of determining who gets to talk and when

- *Give everyone a chance to talk*
- *Don't speak until you are spoken to*
- *Don't monopolize the conversation*
- *Raise a hand when you have a question*
- *Don't interrupt when someone is speaking*

An ideal multiple access protocol should have the following desirable characteristics:

- *Suppose the broadcast channel is of rate R bps.*
- *When only one node has to send data that node has a throughput of Rbps*
- *When M nodes want to transmit each of M nodes has a throughput of R/M bps.*
- *Don't monopolize the conversation*
- *The protocol should be fully decentralized*
- *The protocol should be simple so that it is inexpensive to implement*

Three categories of multiple access protocols:

- *Channel portioning protocol*
- *Random access protocol*
- *Taking –turns protocol*

Module 2

Data Link Layer



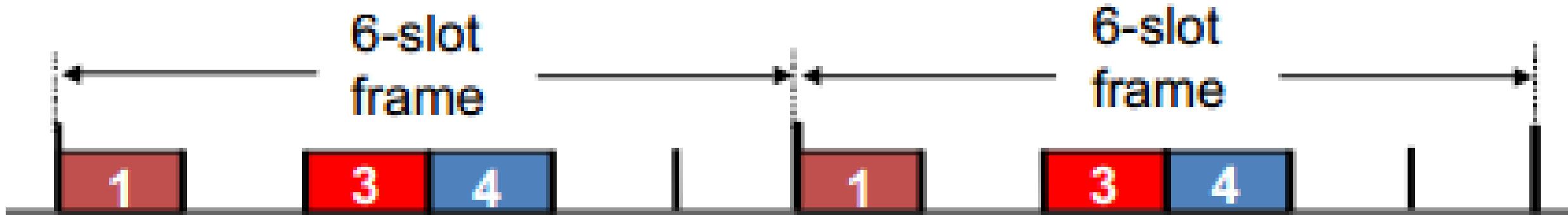
Dr. Sunandita Debnath, IIIT Vadodara

Channel partitioning protocol

- *TDMA (Time Division Multiple Access)*
- *FDMA (Frequency Division Multiple Access)*
- *CDMA (Code Division Multiple access)*

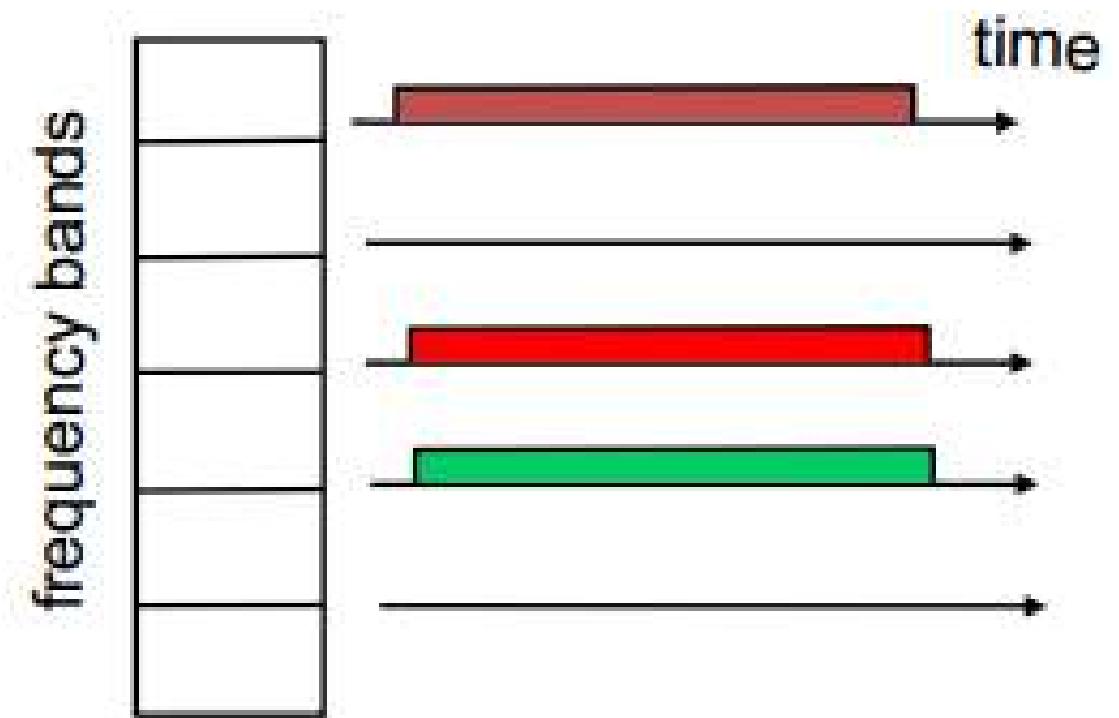
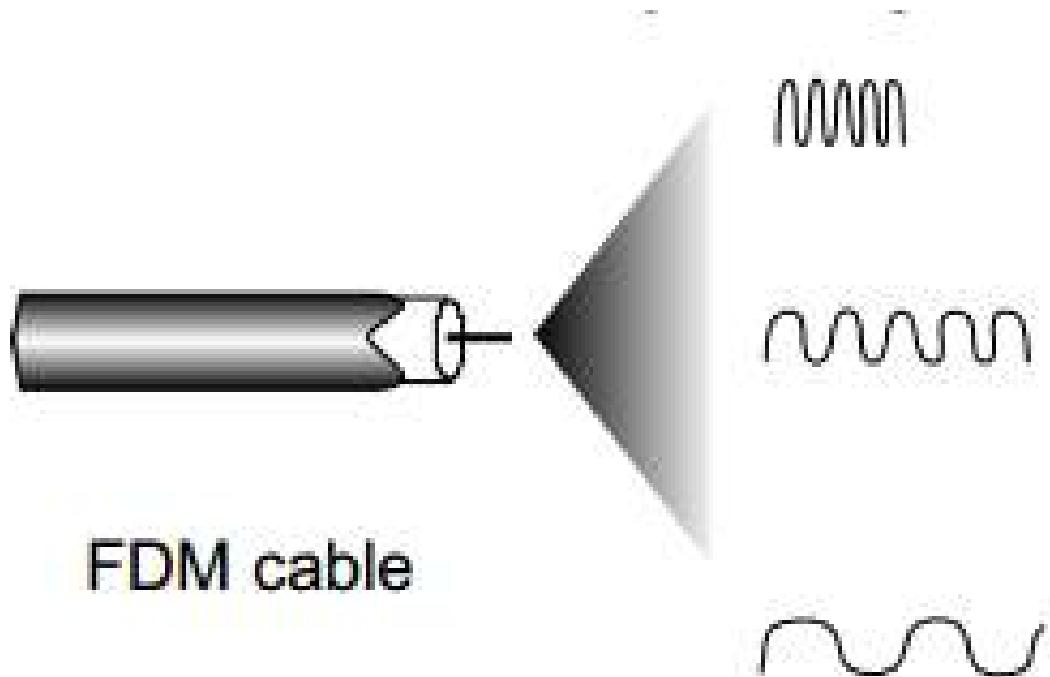
Channel portioning protocol

- *TDMA (Time Division Multiple Access)*



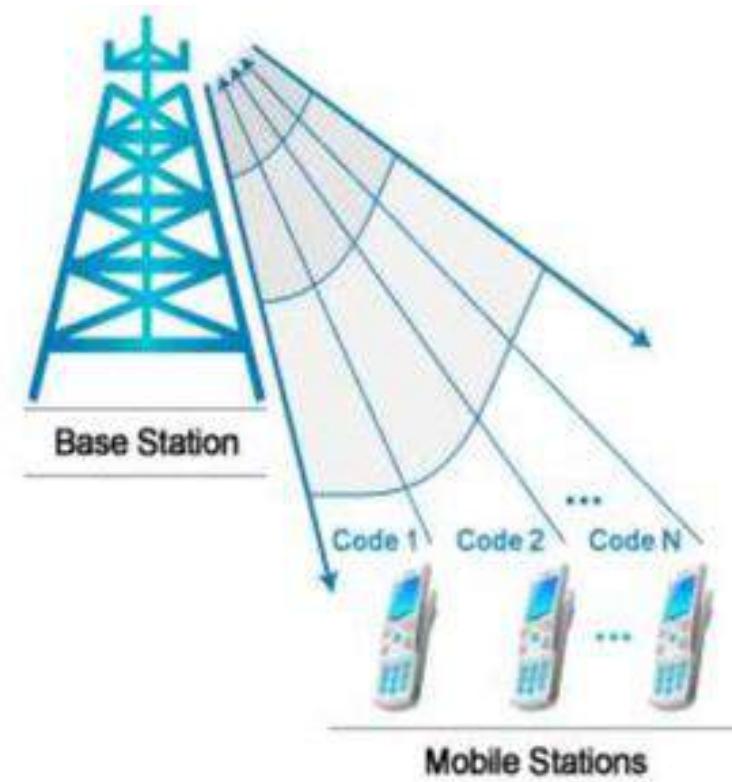
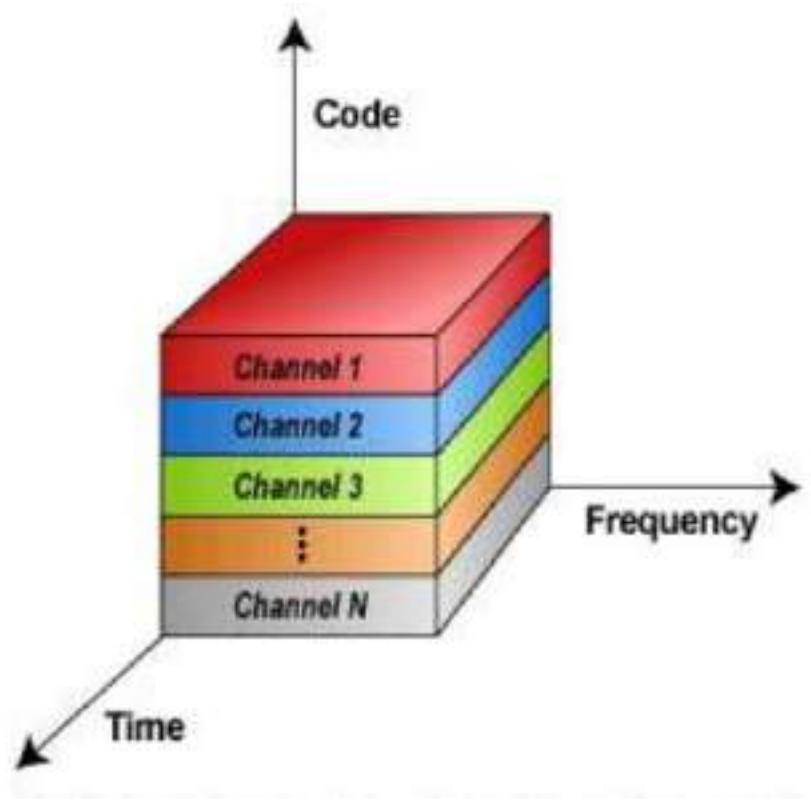
Channel portioning protocol

- *FDM (Frequency Division Multiple Access)*



Channel portioning protocol

➤ **CDMA (Code Division Multiple Access)**



Random access Protocol

➤ *ALOHA*

- Pure ALOHA*
- Slotted ALOHA*

➤ *CSMA(Carrier Sense Multiple access)*

- 1-persistent*
- non-persistent*
- P-persistent*
- O-persistent*

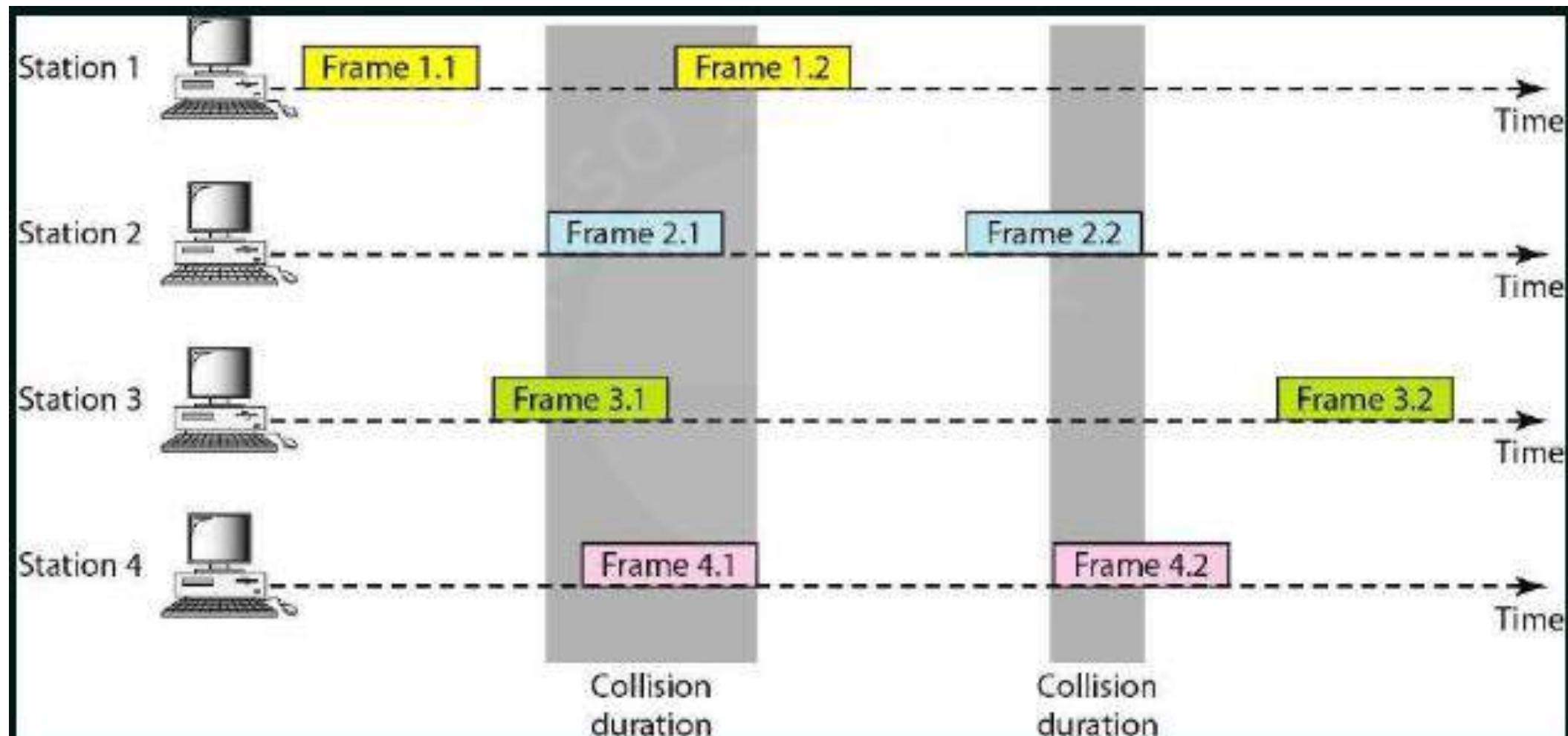
➤ *CSMA/CA*

➤ *CSMA/CD*

Random access Protocol

➤ ALOHA

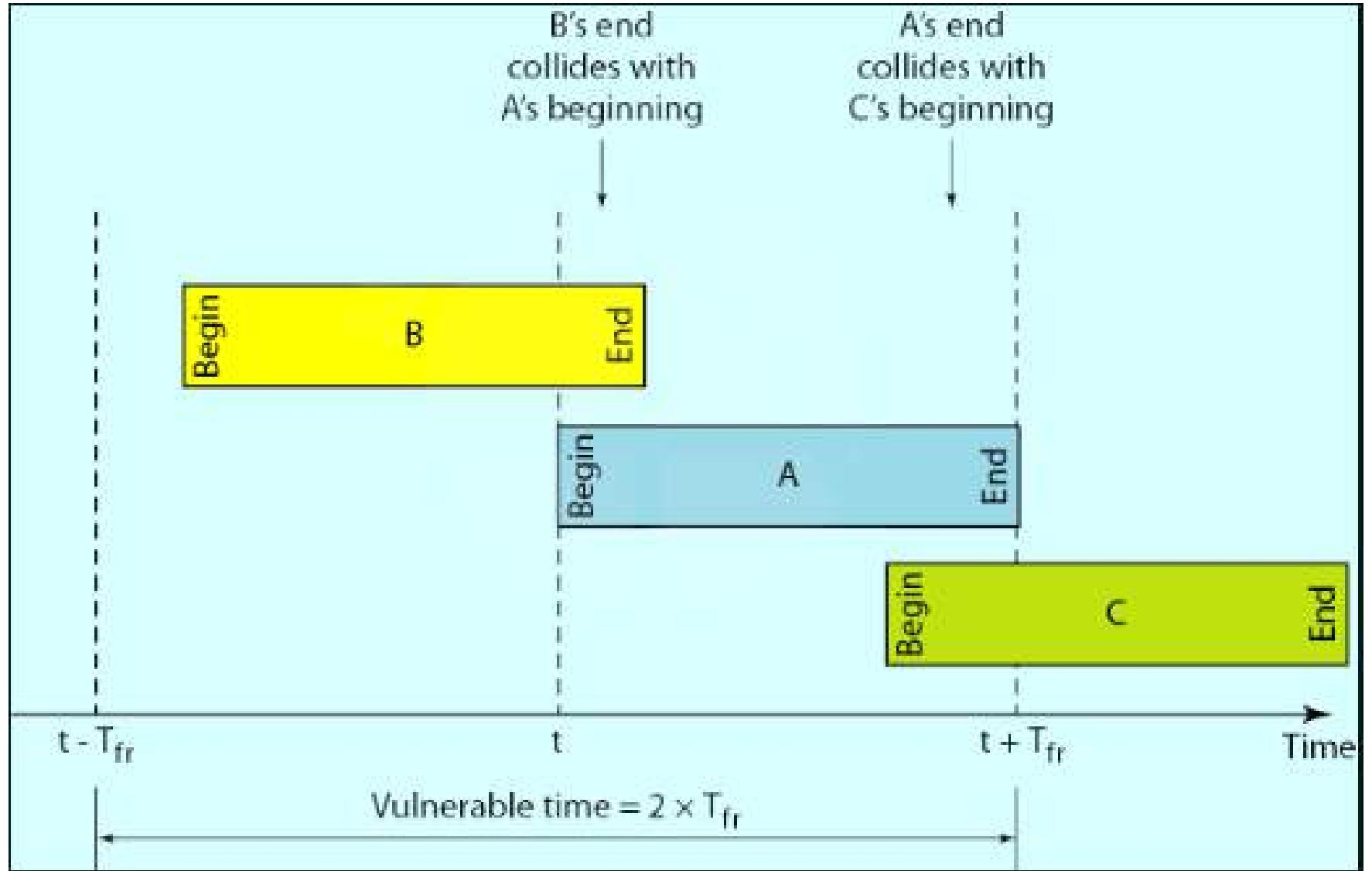
□ Pure ALOHA



Random access Protocol

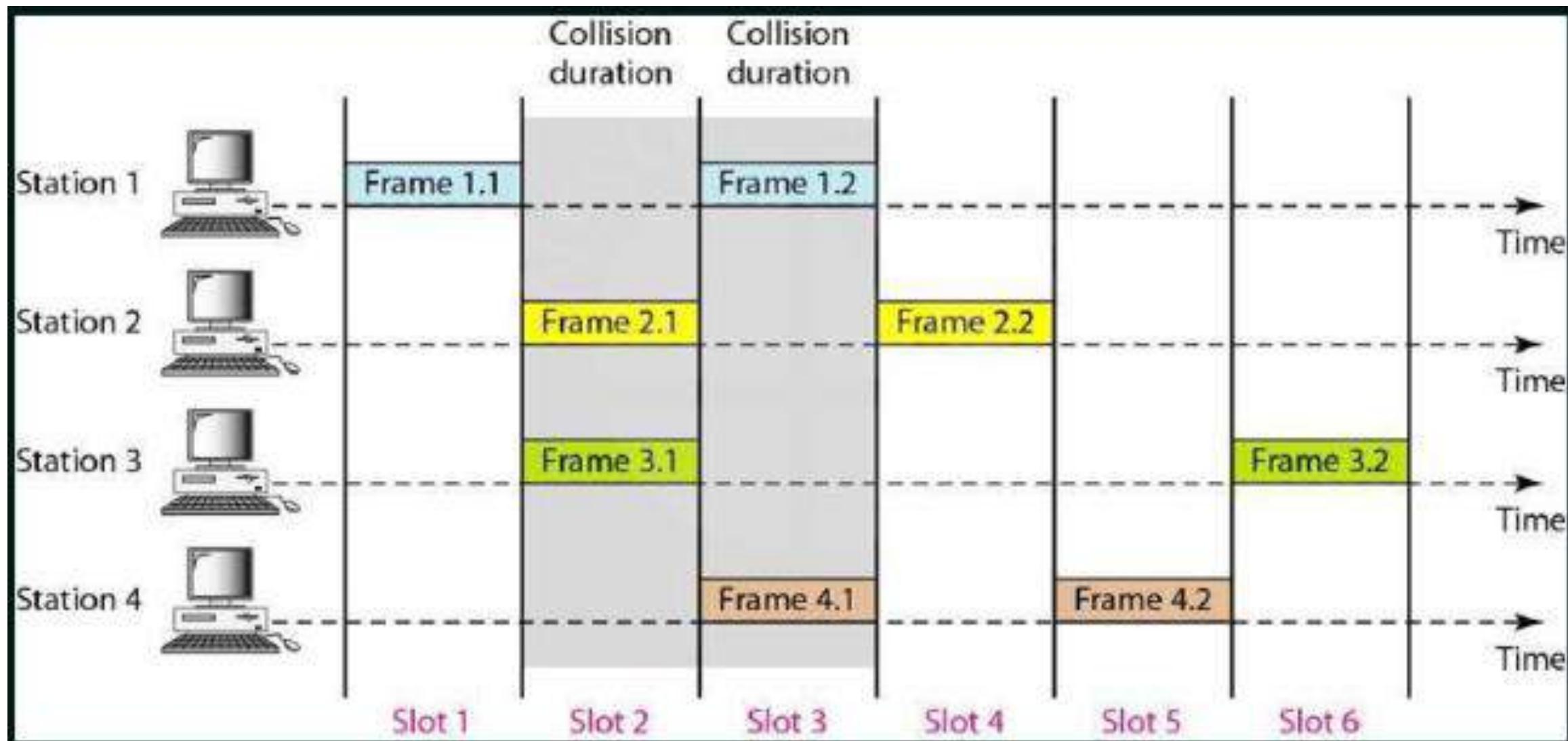
Pure ALOHA

$$\text{Vulnerable time} = 2 \times T_{fr}$$



Random access Protocol

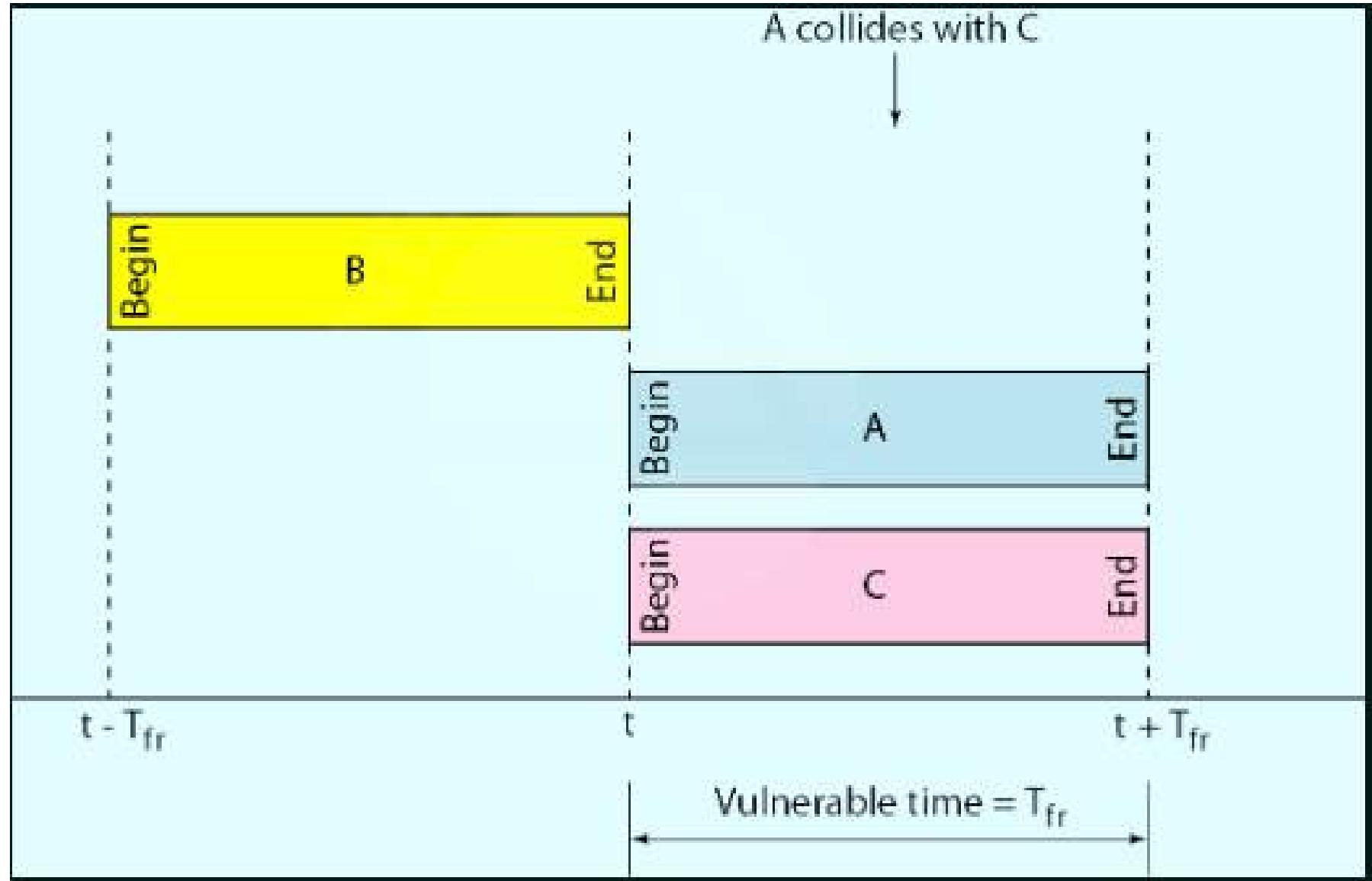
□ Slotted ALOHA



Random access Protocol

Slotted ALOHA

Vulnerable time = T_{fr}



Random access Protocol

Pure Aloha

- Any station can transmit data at any time.
- The time is continuous and not globally synchronized.
- Vulnerable time in which Collision may occur = $2 \times T_{fr}$
- Probability of successful transmission of data packet = $G \times e^{-2G}$
- Maximum efficiency 18.4 % (G=1/2)
- Main advantage is simplicity in transmission.

Slotted Aloha

- Any station can transmit the data at the beginning of any time slot.
- The time is discrete and globally synchronized.
- Vulnerable time in which Collision may occur = T_{fr}
- Probability of successful transmission of data packet = $G \times e^{-G}$
- Maximum efficiency 36.8 % (G=1)
- Main advantage It reduces the number of collision to half and almost double the efficiency.

➤ ***Advantages of slotted Aloha over Channel partitioning***

- In channel partitioning (FDMA and TDMA) when only one active node to transmit , then also it will have access to apportion of the channel e.g. R/N bps not able to transmit at the full rate. In slotted Aloha if only one active user is there then it is able to transmit continuously at the full rate R bps.
- But in slotted Aloha un-wasted slots are the only slot in which exactly one node transmits. The efficiency of slotted Aloha is when there are a large number of active users and each of them always having a large no. of frames to transmit.

Module 2

Datalink Layer



Dr. Sunandita Debnath, IIIT Vadodara

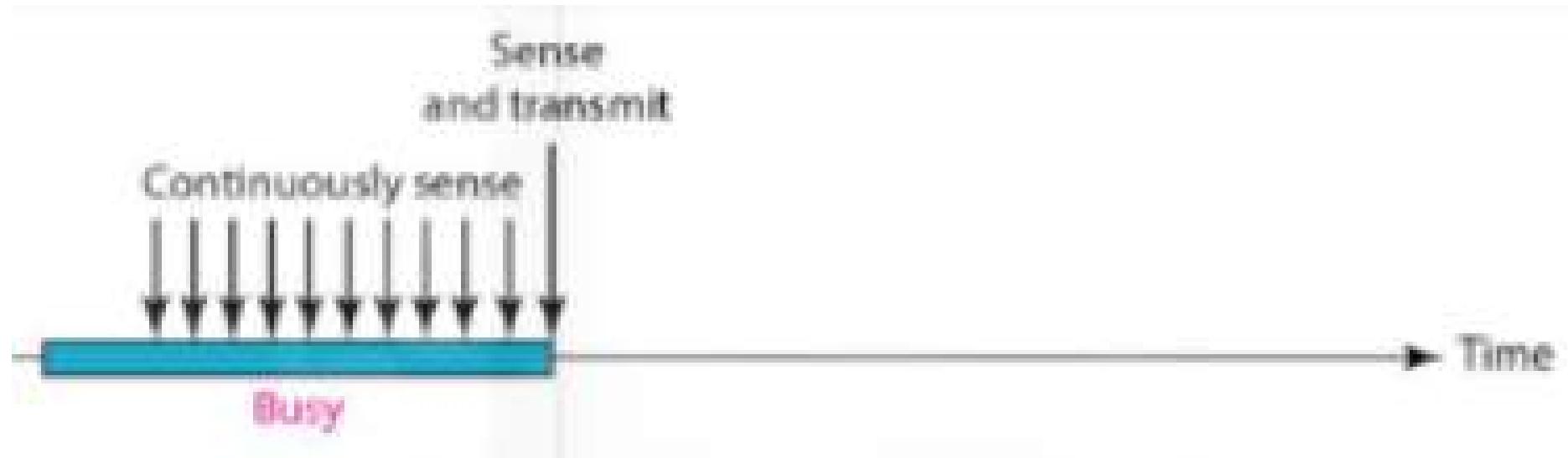
➤ CSMA(*Carrier Sense Multiple access*)

- *The disadvantages of pure and slotted Aloha has been overcomed in CSMA In Aloha the node's decision to transmit is made independently of the activity of the other nodes attached to the broadcast channel.*
- *CSMA is based on channel (carrier) sensing mechanism.*
 - *Listen before speaking-This is called carrier sensing, a node listens to the channel before transmitting. If a frame from another node is currently being transmitted into the channel, a node then waits until it detects no transmission for short amount of time and then begin transmission.*
 - *If someone else begins talking at the same time, stop talking- This is called collision detection. A transmitting node listens to the channel while it is transmitting. If it detects that another node is transmitting an interfering frame, it stops transmitting and waits for a random amount of time before repeating the sense-and –transmit-when-idle cycle*

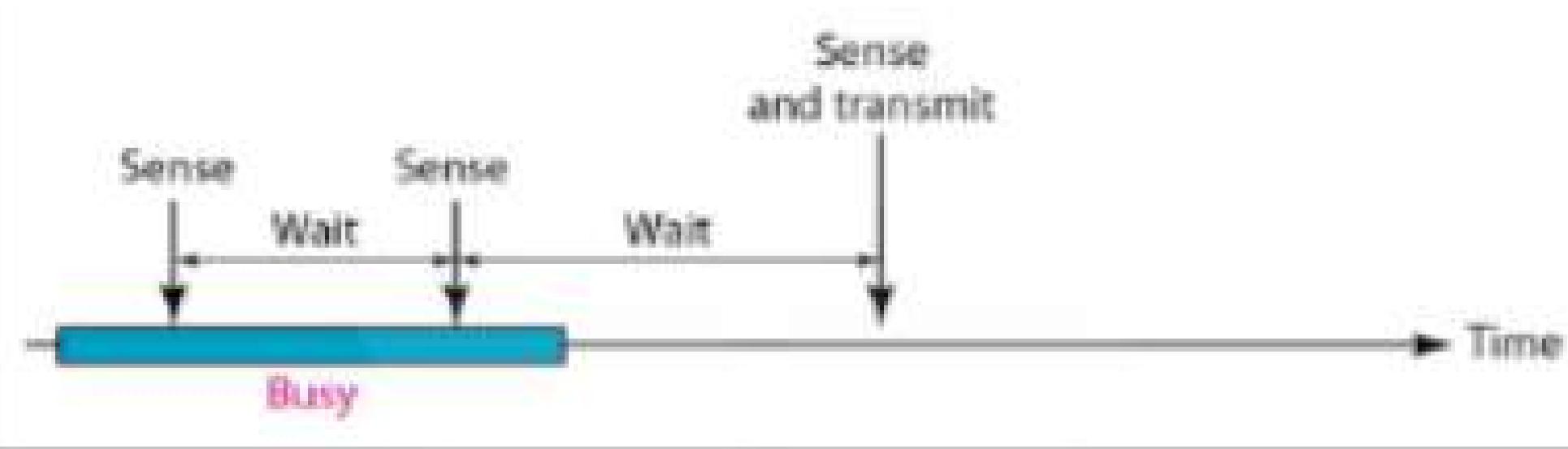
➤ CSMA(*Carrier Sense Multiple access*)

1-persistent	non-persistent	P-persistent
<ul style="list-style-type: none">Before sending the data, the station first listens to the channel to see if anyone else is transmitting at that moment. If the channel is idle the station transmits a frame.If busy then it senses continuously until it becomes idle.Since the station transmits the frame with probability 1 when the channel is idle, the scheme is called 1-persistent CSMA.	<ul style="list-style-type: none">Before sending a frame, a station senses the channel. If no one else is sending the station begins sending.However, if a channel is busy, the station does not continuously sense it for the purpose of seizing immediately upon detecting the end of previous transmission.Instead it waits for a random amount of time and then repeats the algorithm.Consequently this algorithm leads to better channel utilization but longer delays than 1-persistent CSMA.	<ul style="list-style-type: none">It applies to a slotted channel. When a station becomes ready to send it senses the channel.If it is idle it transmits with the probability P. and it defers with a probability $Q = (1 - P)$ until the next slot.If that slot is idle , it either transmits or defers again with probability P & Q. This process is repeated until either the frame is has been transmitted or any other station has begin transmission.In the later case the unlucky station acts like there had a collision and waits for random

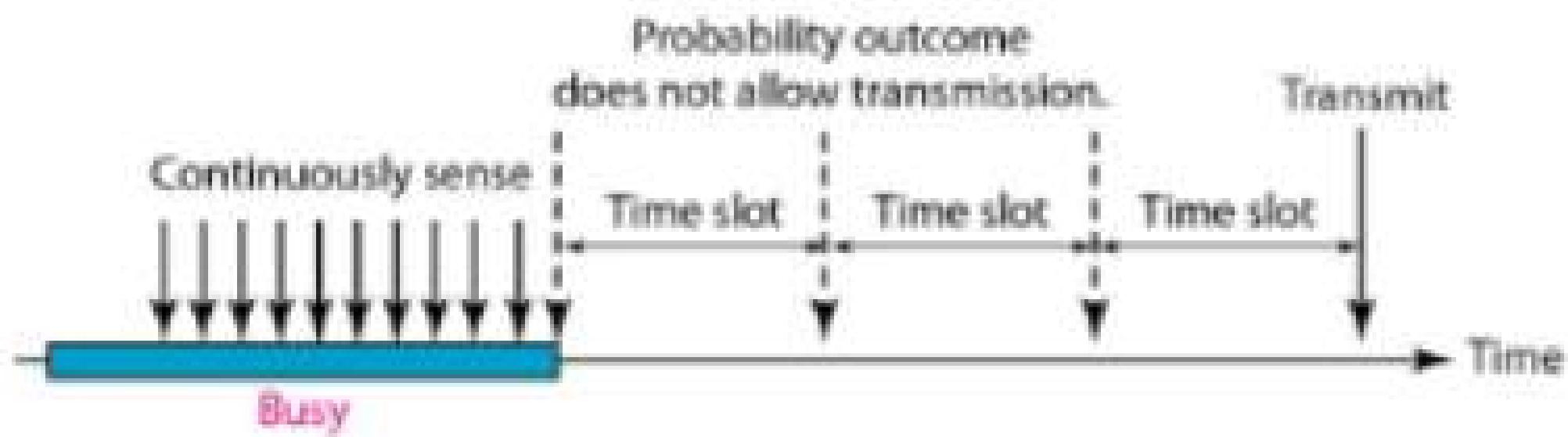
1-persistent



non-persistent



P-persistent

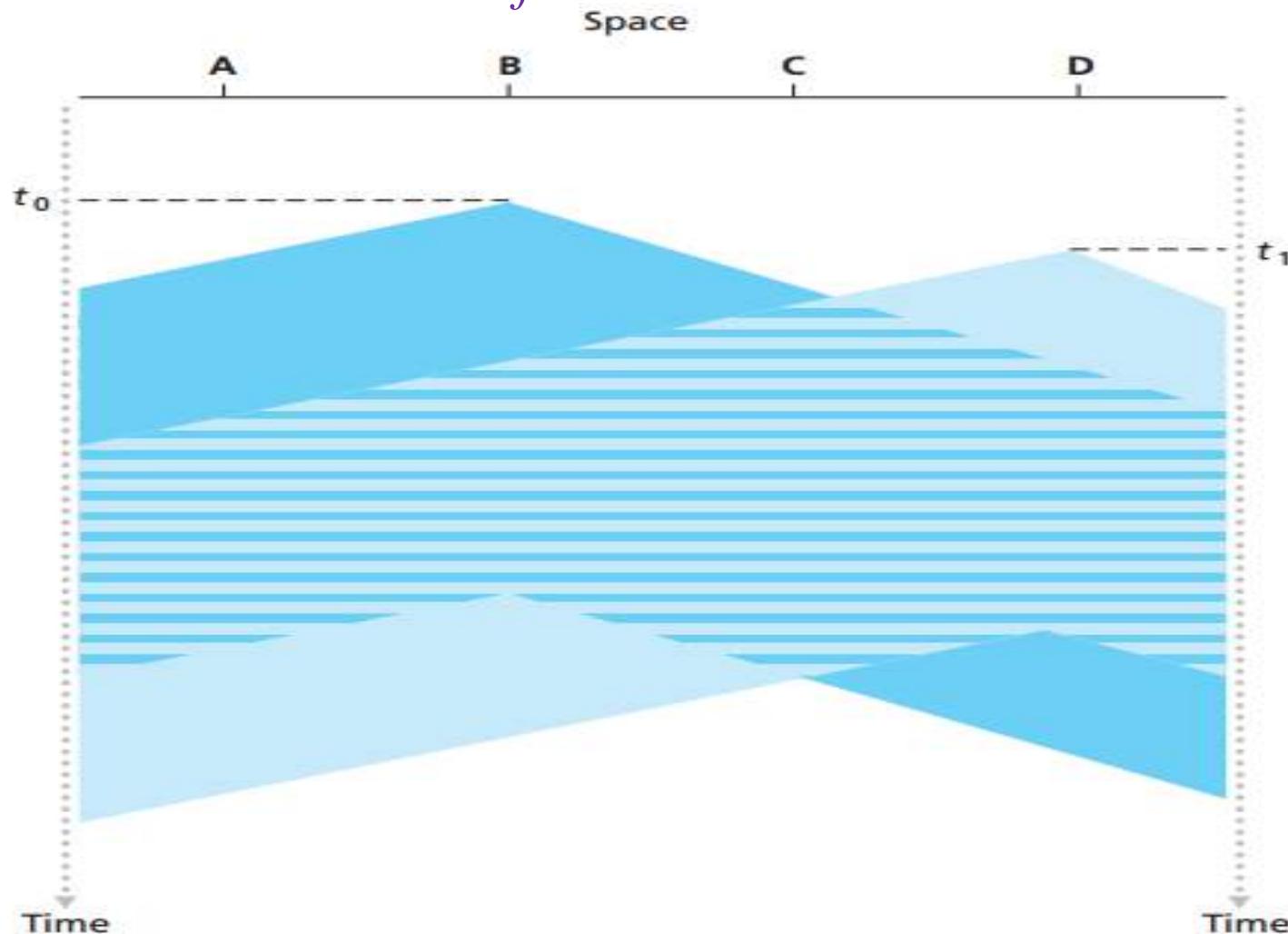


O-persistent

Each node is assigned a transmission order by a supervisory node

The effect of propagation delay in CSMA

➤ Sender B started transmission at t_0 as it senses the medium is idle. As the propagation delay is nonzero at time t_1 ($t_1 > t_0$), node D senses the medium is idle and begin its transmission and after a short interval of time B's frame interfere with D's frame. So longer the end-to-end propagation delay more will be the chances of collision.



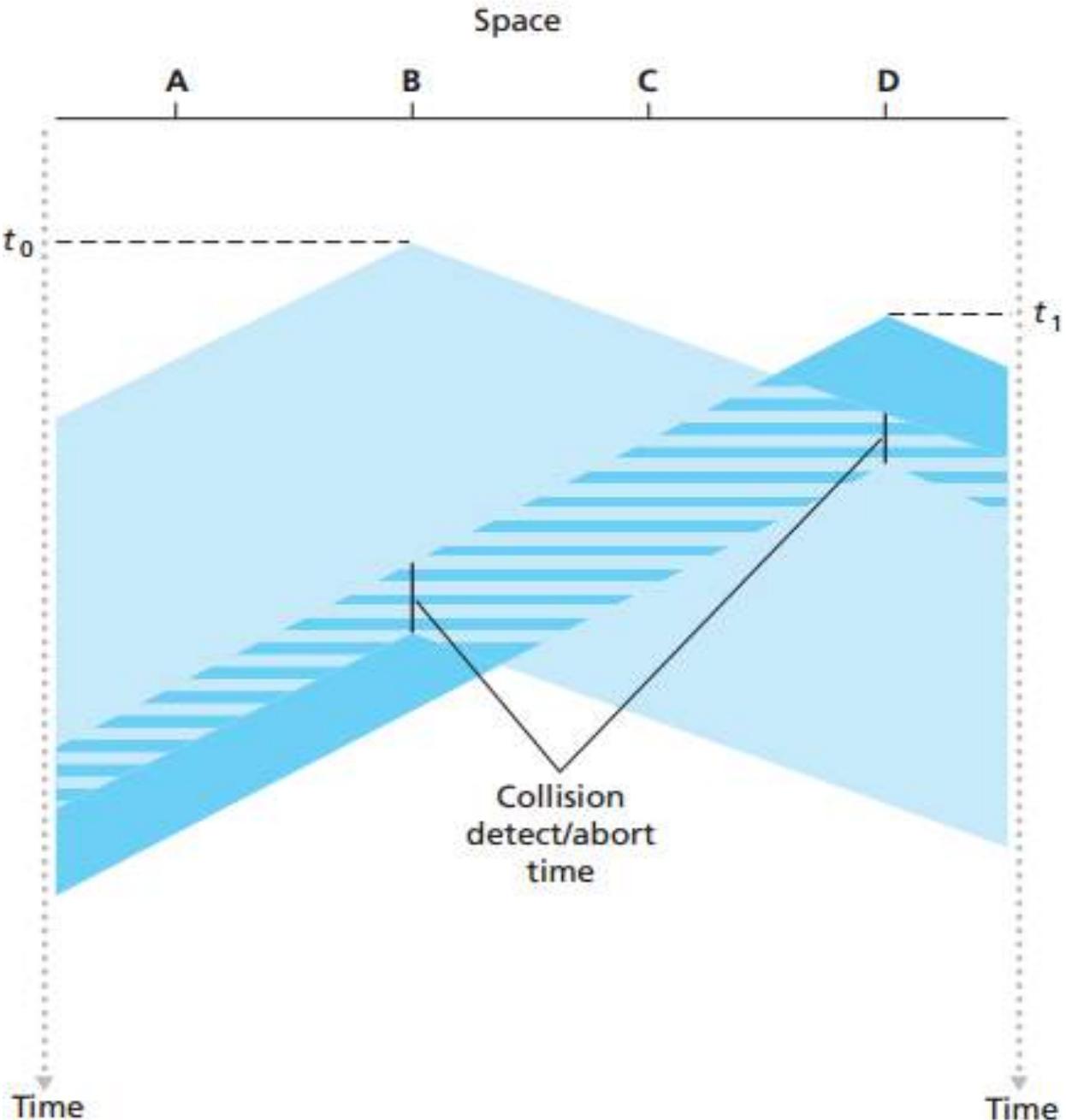
CSMA(Carrier Sense Multiple access)

CSMA/CD

➤ If two stations senses the channel is idle and begin transmitting simultaneously, then both will detect collision almost immediately.

➤ As soon as it detects a collision both the sender ceases transmission. Quickly terminating damaged and corrupted frames from transmitting saves time and bandwidth.

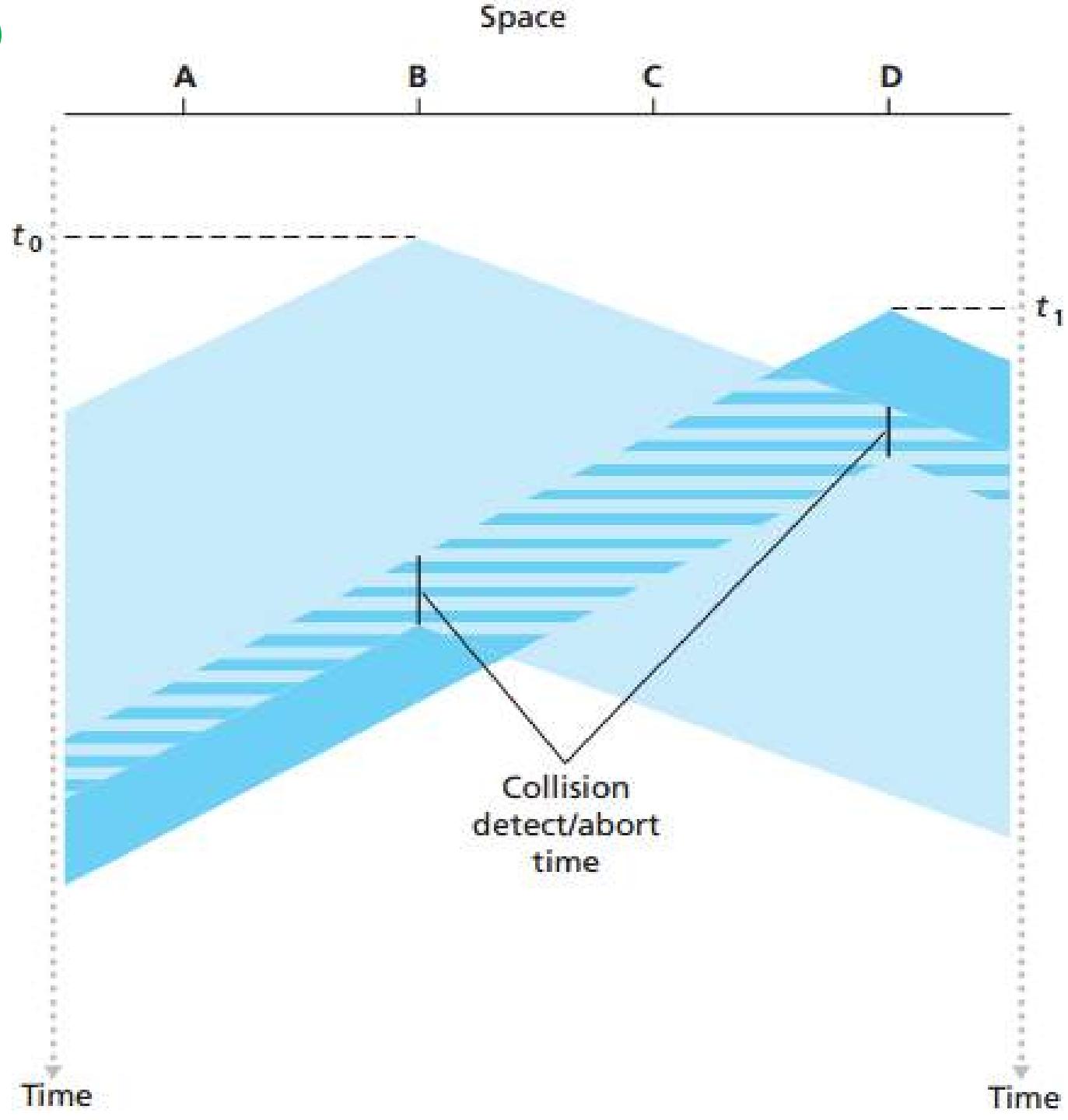
➤ CSMA/CD is used in LANs and Ethernet



CSMA(Carrier Sense Multiple access)

CSMA/CD

- After aborting the transmission. Both the senders wait for a random amount of time.
- If both the stations waits for the same amount of time then again they will collide and continue colliding forever.
- Two cases to be considered:
 - If the interval is large and number of colliding node are small, nodes are likely to wait a large amount of time before repeating the transmission again.
 - If the interval time is small and large number of colliding nodes are there then the randomly chosen time to be nearly close and the nodes will collide again.



CSMA(*Carrier Sense Multiple access*)

Binary Back-off Algorithm for CSMA/CD

- It is used in Ethernet.
- Suppose a frame has already experienced n collisions, then this sender will chooses the vale K at random K belongs to $(0,1,2 \dots, 2^n - 1)$.
- Thus the more numbers of collision the larger the interval from which the K value will be chosen.
- Suppose a sender attempts to frame for the first time and detects a collision then, $n = 1$, so $2^1 - 1 = 1$. Therefore the range of $k \in (0,1)$. So it chooses $K = 0$ with probability $\frac{1}{2}$ and chooses 1 with probability $\frac{1}{2}$.
- Thus, the size of the sets from which K is chosen grows exponentially with the number of collisions; for this reason this algorithm is referred to as binary exponential backoff.
- The efficiency of CDMA/CD is given by

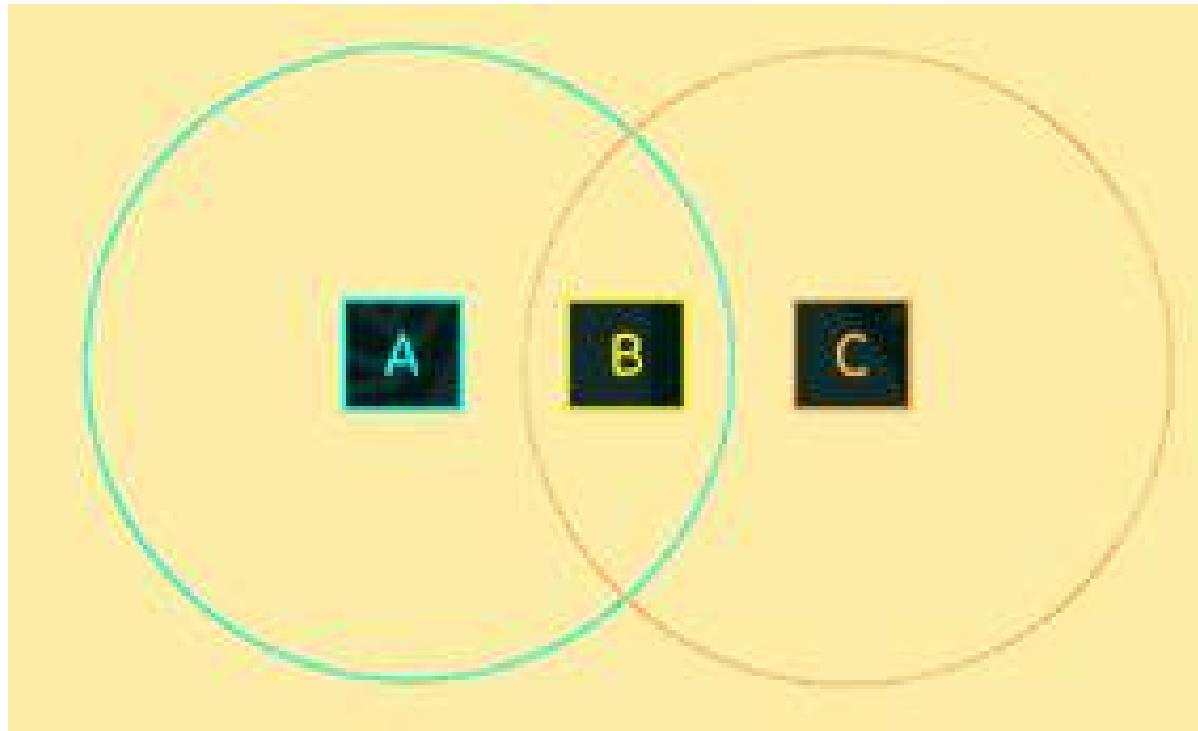
$$\text{Efficiency} = \frac{1}{1 + 5d_{prop}/d_{trans}}$$

CSMA(*Carrier Sense Multiple access*)

CSMA/CA (Collision Avoidance)

- *It is used for wireless communication.*
- *CSMA/CA is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by beginning transmission only after channel is sensed to be idle.*
- *I is particularly important for wireless networks. Where the collision detection of the alternative CSMA/CD is not possible due to wireless transmitters desensing their receivers during packet transmission.*
- *CSMA/CA is unreliable because of hidden node problem and exposed terminal problem.*
- *Solution is RTS (request to send)/CTS (clear to send)*
- *The access method used in IEEE 802.11 (WiFi) is CSMA/CA.*

Hidden Terminal Problem



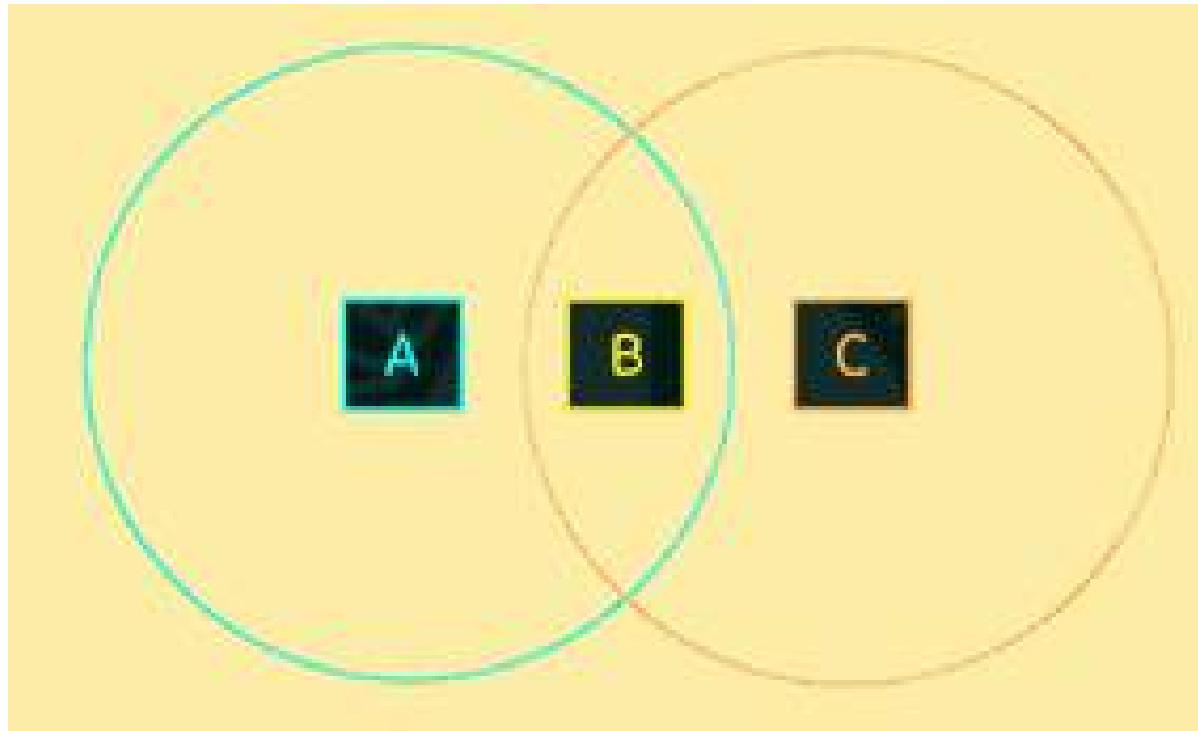
Suppose both A and C want to communicate with B and so they each can send it a frame

➤ *A and C are unaware of each other since their signals do not reach that far in other words they are not in the sensing range of each other.*

➤ *These two frames collide with each other at B (but unlike Ethernet neither A or C is aware of this collision).*

➤ *A and C are hidden nodes with respect to each other.*

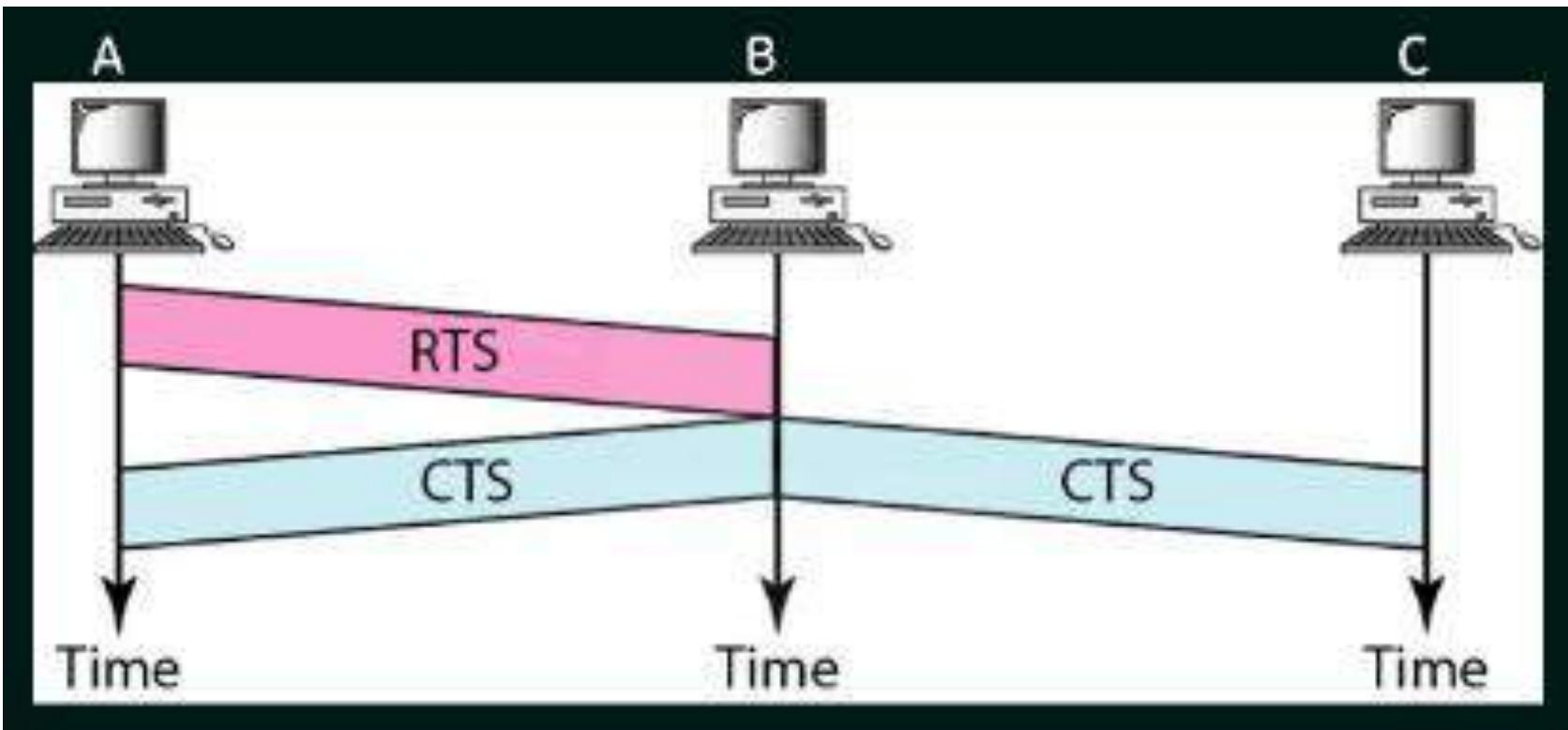
MACA Protocol



This hidden node problem is solved using MACA protocol. Suppose both A and C want to communicate with B and so they each can send it a frame

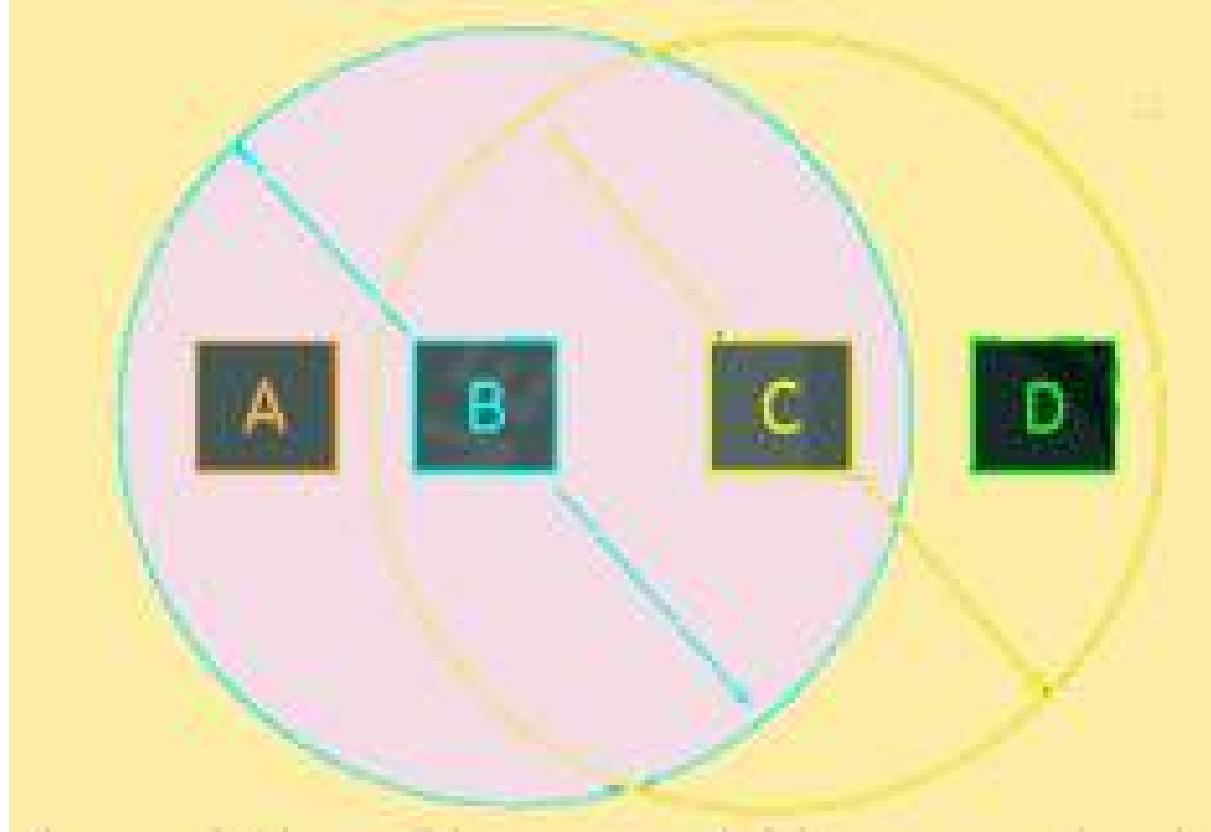
- *A and C are unaware of each other since their signals do not reach that far in other words they are not in the sensing range of each other.*
- *These two frames collide with each other at B (but unlike Ethernet neither A or C is aware of this collision).*

MACA Protocol



Station C doesn't hear RTS from A, but it does hear CTS from B, so it know something is up.

Exposed Terminal Problem



Suppose B is sensing to A. Node C is aware of this communication because B is in range of C i.e. it can hear B's transmission.

➤ *It would be mistake to C to conclude that it cannot transmit to D or anyone just because it can hear B's transmission.*

➤ *IF C wants to transmit to D , this is not a problem since C's transmission to D will not interfere with A's ability to transmit or receive from B.*

CSMA/CA –Two algorithms are addressed in IEEE 802.11 with:

- **MACA (Multiple Access with Collision Avoidance)**
- **MACAW (MACA for Wireless LANs)**

MACA

- In MACA sender and receiver exchange control frames with each other before the sender actually transmits any data.
- This exchange informs all nearby nodes that a transmission is about to begin
- Sender transmits a RTS (Request to Send) frame to the receiver
 - RTS frame includes a field that indicate how long the sender wants to hold the medium/ channel i.e. the length of the data frame be to transmitted.
- Receiver replies with a CTS (Clear to Send) frame
 - This CTS frame is broadcast by the receiver and also includes the length of the frame which is informed by the sender while asking for request to send.
- Any node which hears the CTS frame knows that it is close to the receiver, therefrom refrained from transmitting (i.e. cannot transmit) for the period of time it takes to send a frame of the specified length.

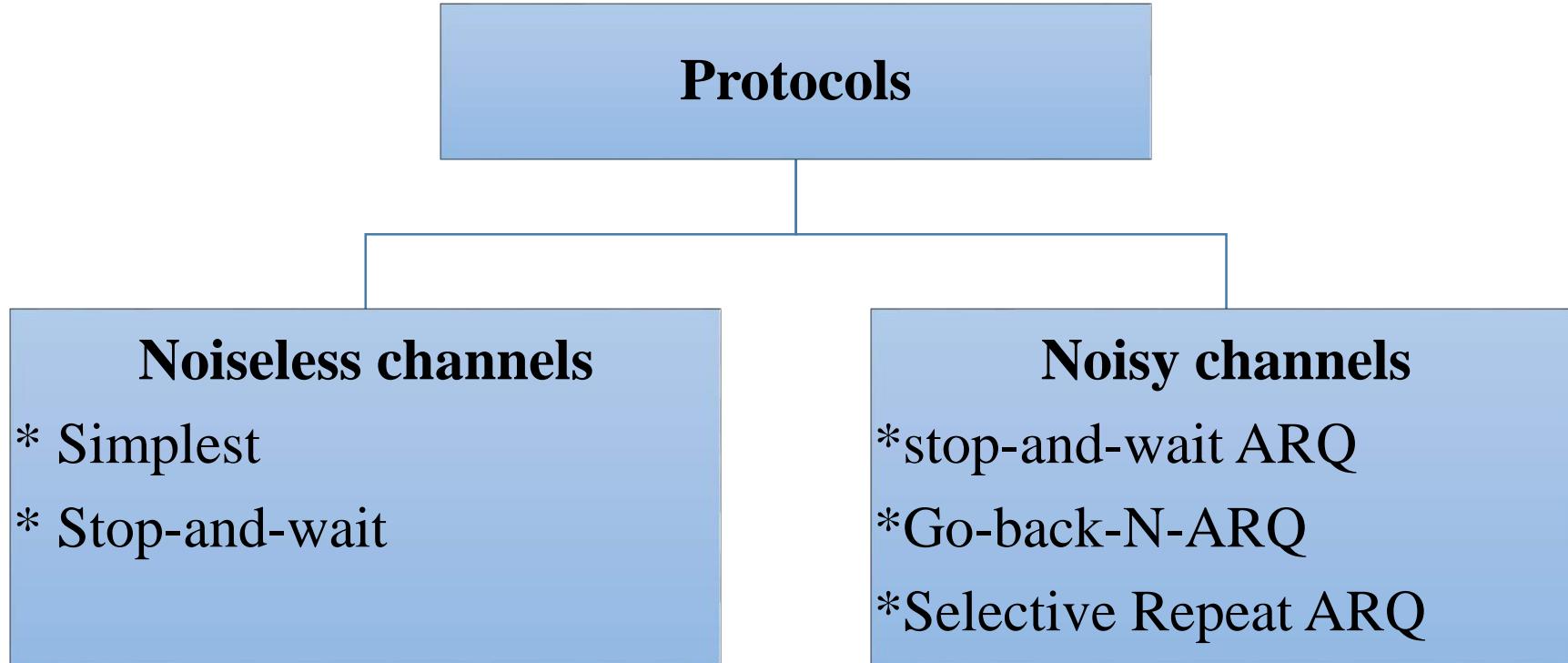
MACA

- Any node that hears the RTS frame but not the CTS frame it gets to know that it is not close enough to the receiver to interfere with it and so free to transmit to any other node.

MACAW

- The idea of using CK (acknowledgement)A in MACA is proposed in MACAW: MACA for Wireless LANs.
- Receiver sends a ACK to the sender after successfully receiving a frame.
- As this ACK is also a broadcast message, all nodes must wait till this ACK before trying to begin a new transmission.
- If two or more nodes detect an idle link and try to transmit an RTS at the same time
 - This RTS frame will collide with each other
 - 802.11 does not support collision detection
 - So the sender realizes the collision has happened when they are not receiving an CTS after a period of time from the receiver node.
 - In this case they both wait a random period of time before trying again
 - The amount of time a given node must wait is defined by the same exponential backoff algorithm used on the Ethernet.

Flow control



Stop and wait protocol

- Stop-and-wait protocol is data link layer protocol for transmission of frames over noiseless channels.
- It provides unidirectional data transmission with flow control facilities but without error control facilities.
- After transmitting one frame, the sender waits for an acknowledgement before transmitting the next frame.

➤ **Sender side :**

Rule 1: send one data frame at a time

Rule 2: Send the next frame only after receiving ACK for the previous one.

➤ **Receiver side:**

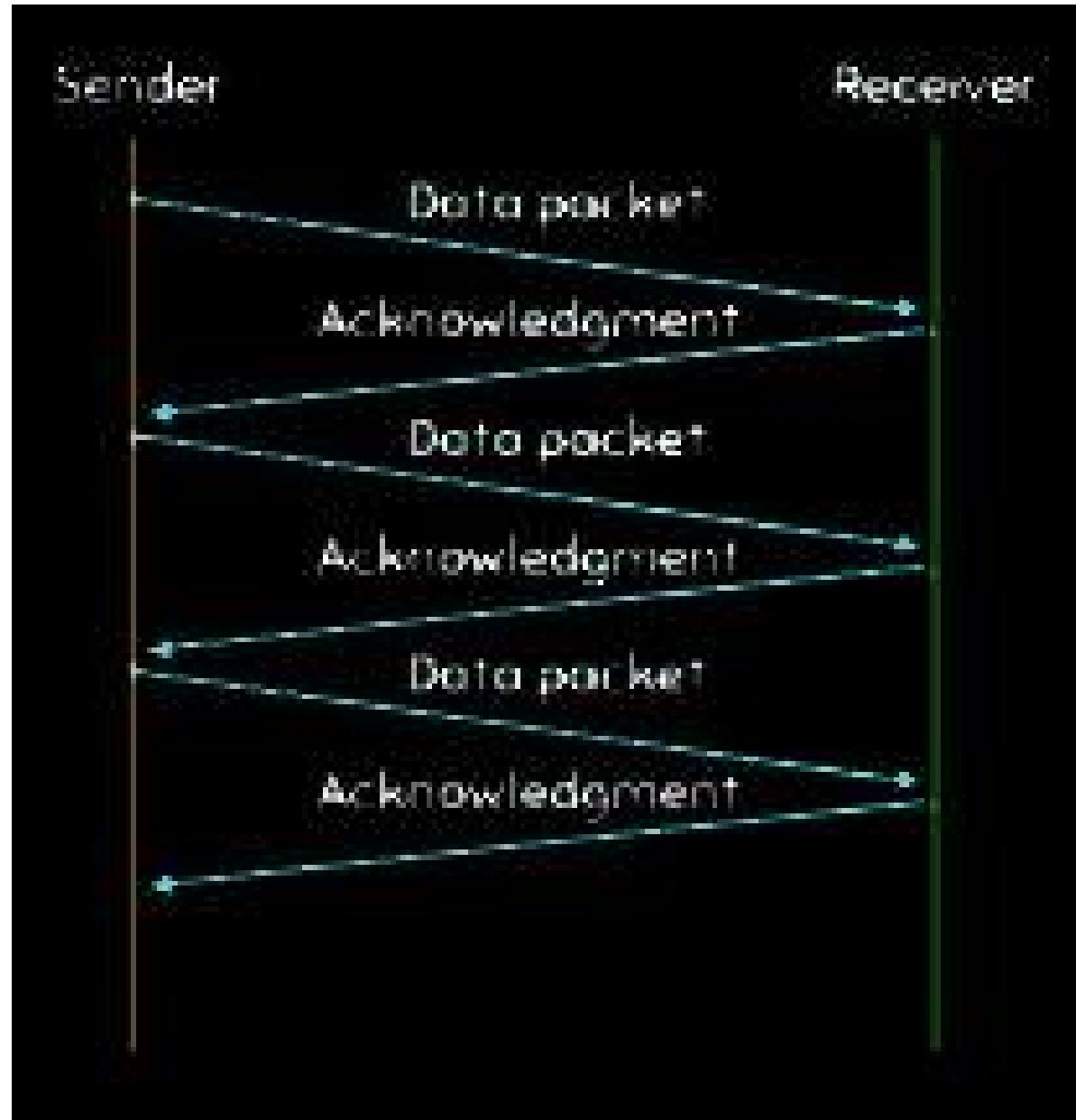
Rule 1: Receive and consume frame send one data frame at a time

Rule 2: After consuming frame ACK need to be sent (Flow control)

Stop and wait protocol

The disadvantage of this protocol is if the sender has a large number of frames say 1000 frames then it has to send only one frame at a time and waits for the ACK each time.

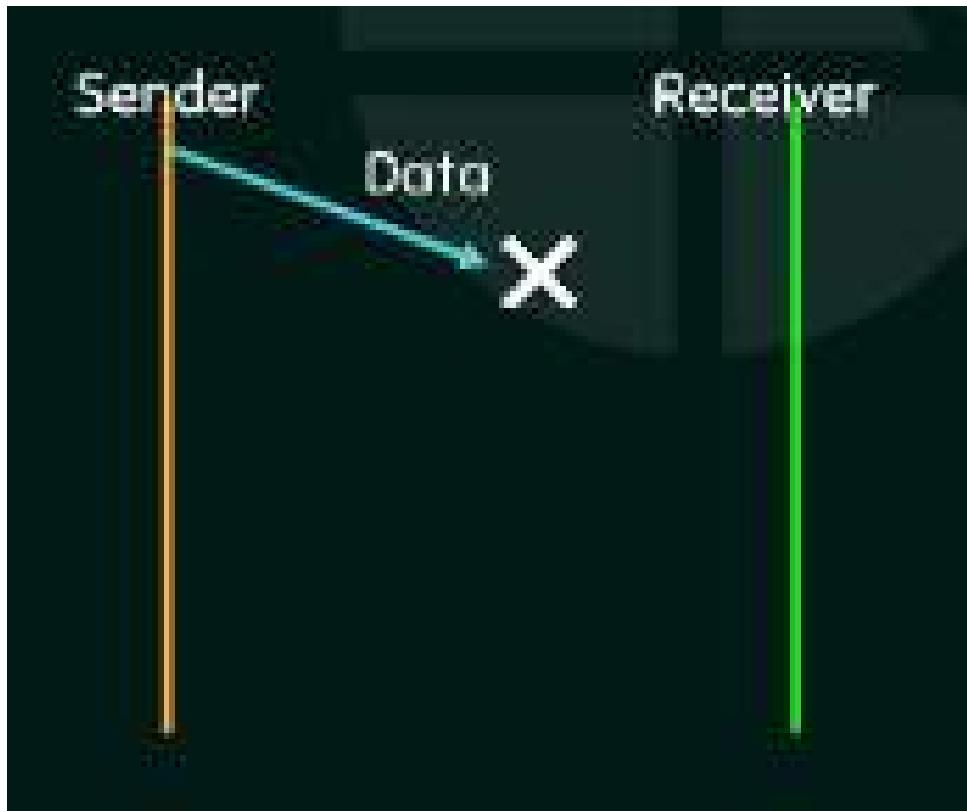
- Problem due to lost frame
- Problem due to lost ACK
- Problem due to delayed frame/ACK



Stop and wait protocol

Problem due to lost frame

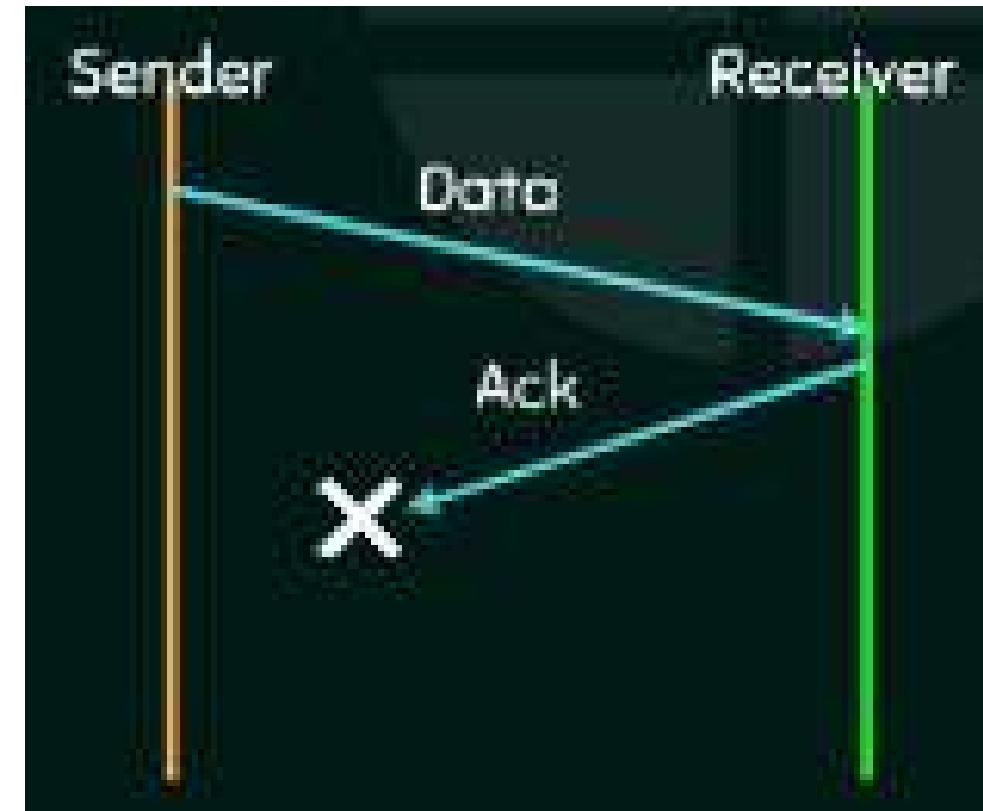
- Sender waits for ACK for an infinite amount of time
- Receiver waits for data for an infinite amount of time



Stop and wait protocol

Problem due to lost ACK

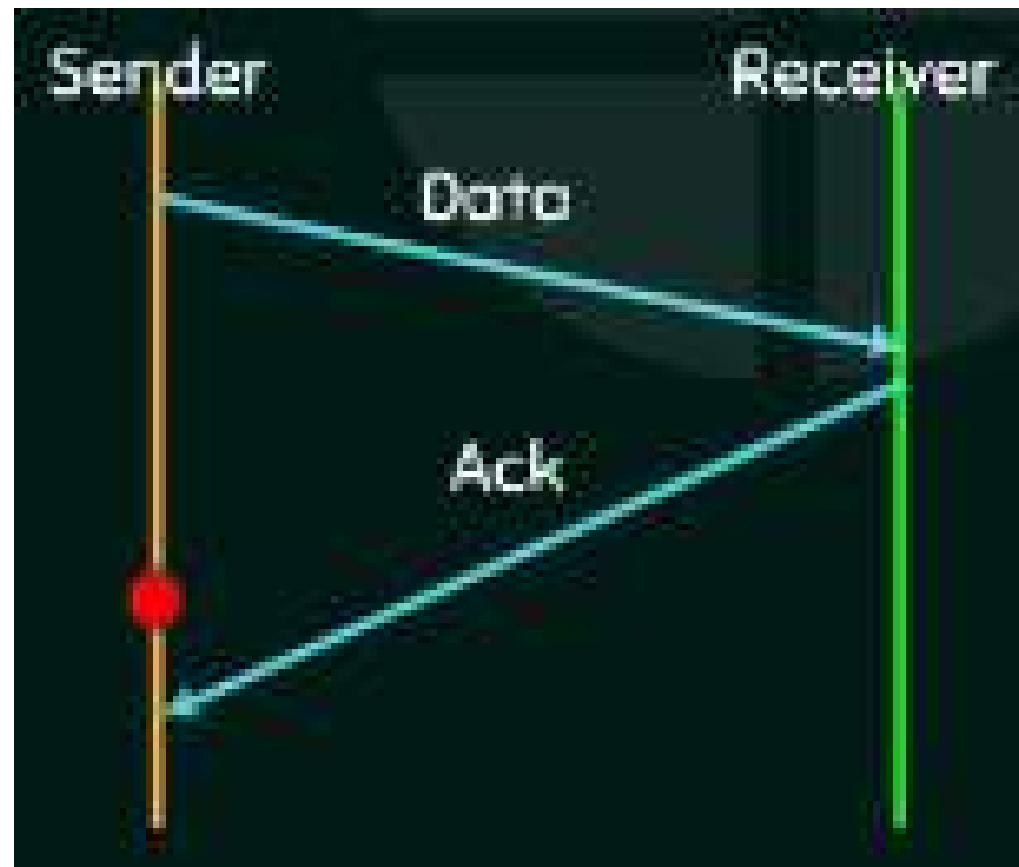
- Sender waits for an infinite amount of time for ACK. So there is an infinite delay for the next frame in the queue to be transmitted.



Stop and wait protocol

Problem due to delayed frame/ACK

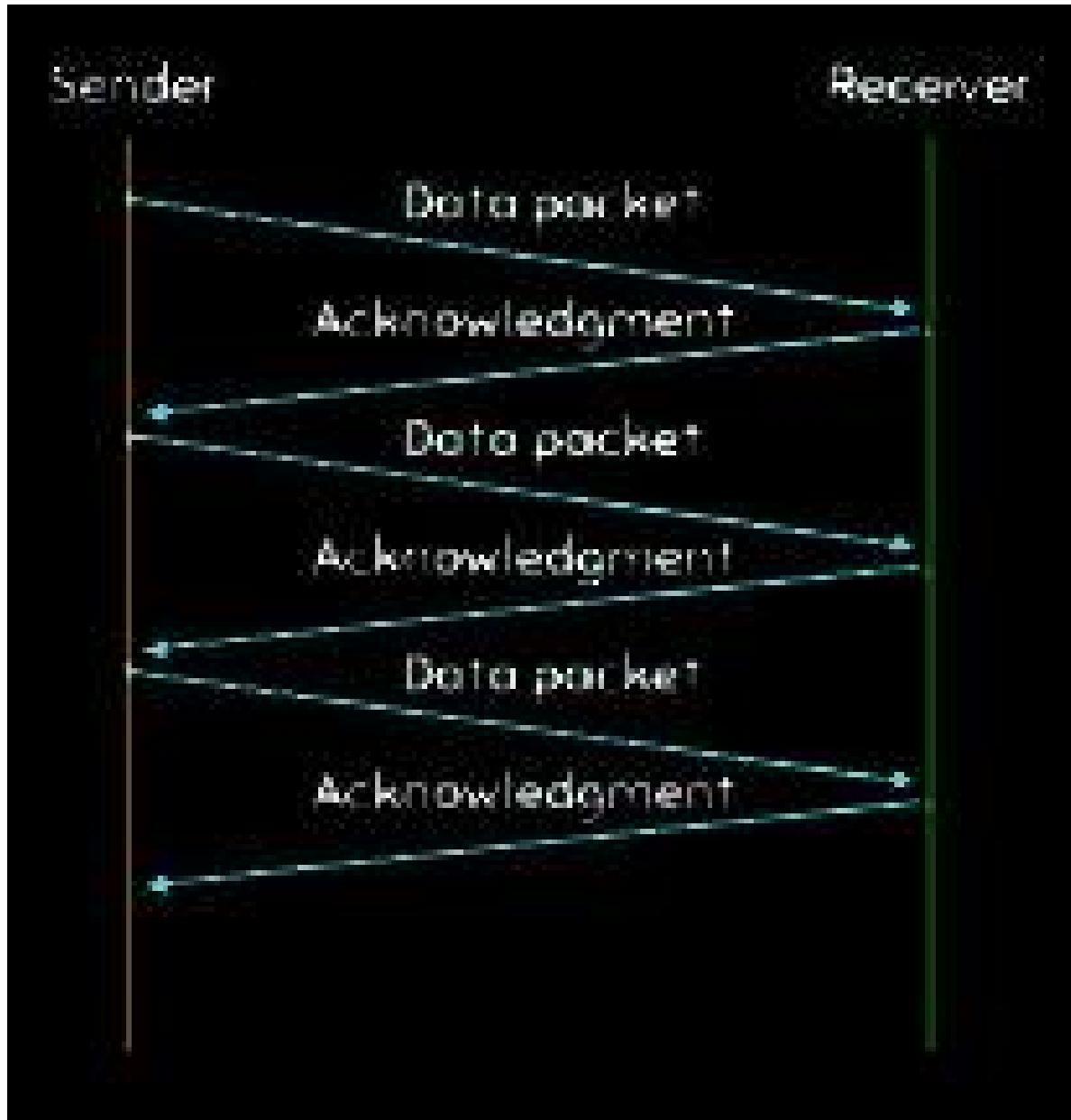
- After timeout at sender side, a delayed ACK might be wrongly considered as ACK of some other data frames.



Stop and wait protocol

The disadvantage of this protocol is if the sender has a large number of frames say 1000 frames then it has to send only one frame at a time and waits for the ACK each time.

- Problem due to lost frame
- Problem due to lost ACK
- Problem due to delayed frame/ACK

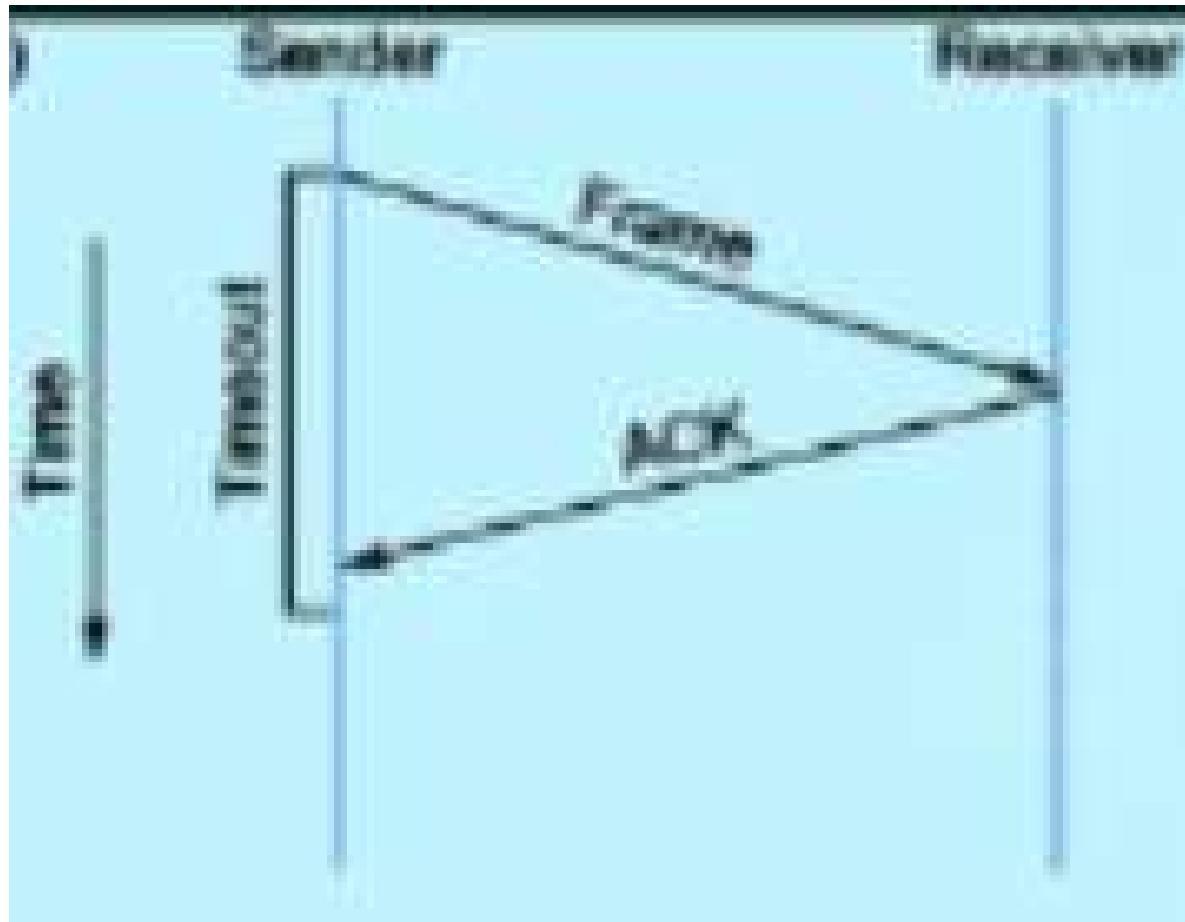


Stop and wait ARQ protocol

- After transmitting one frame, the sender waits for an acknowledgement before transmitting the next frame.
- If the acknowledgement does not arrive after a certain period of time the sender times out and retransmits the original frame.
- **Stop and wait ARQ = Stop and wait + Timeout Timer +Sequence number**

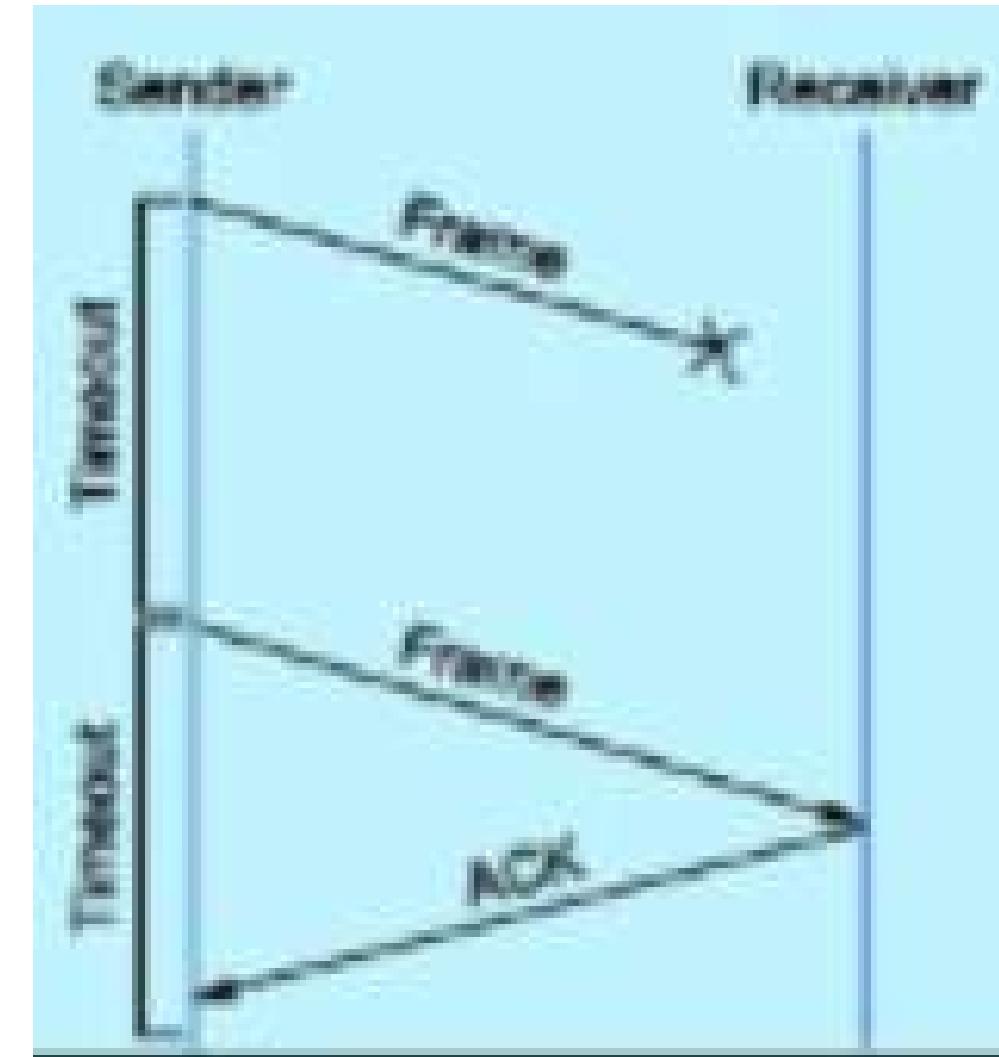
Stop and wait ARQ protocol

ACK is received before the timer expires



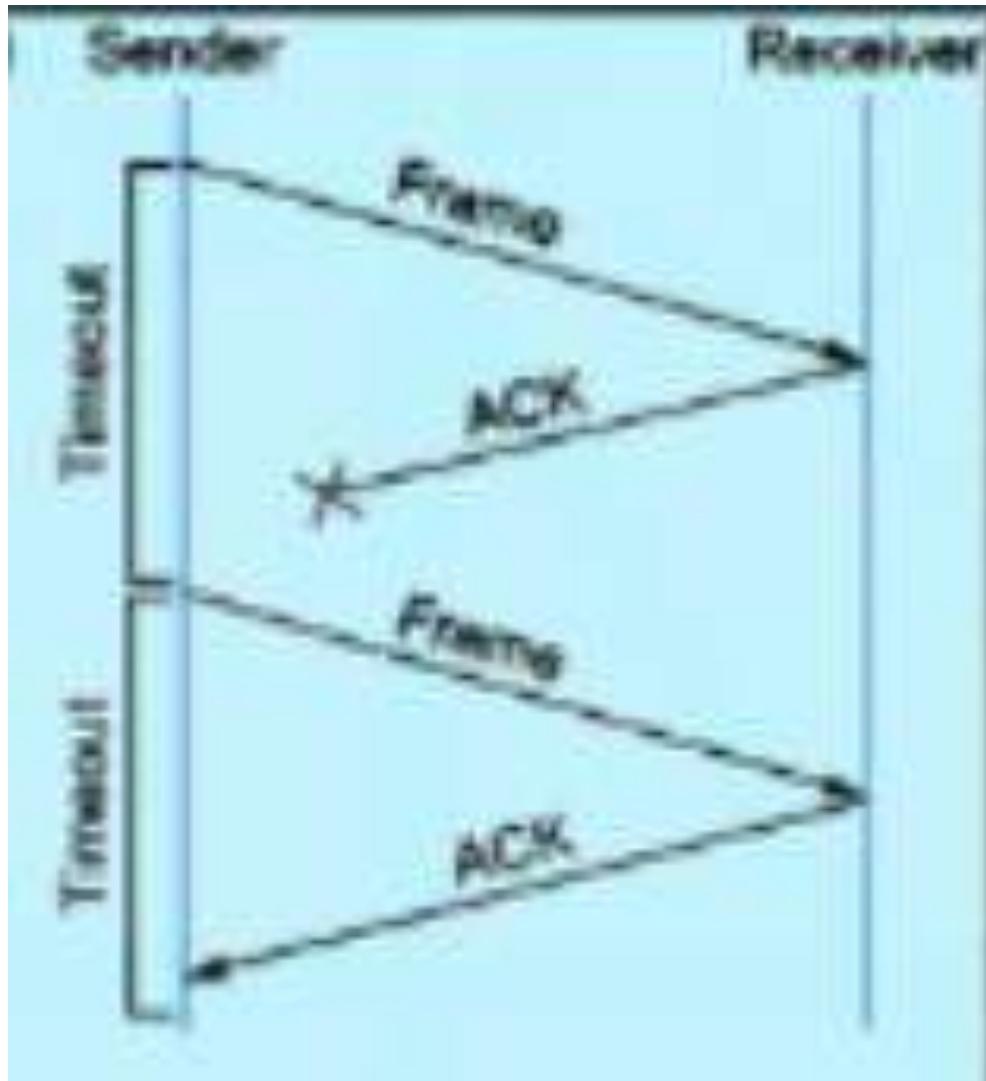
Stop and wait protocol

The original frame is lost



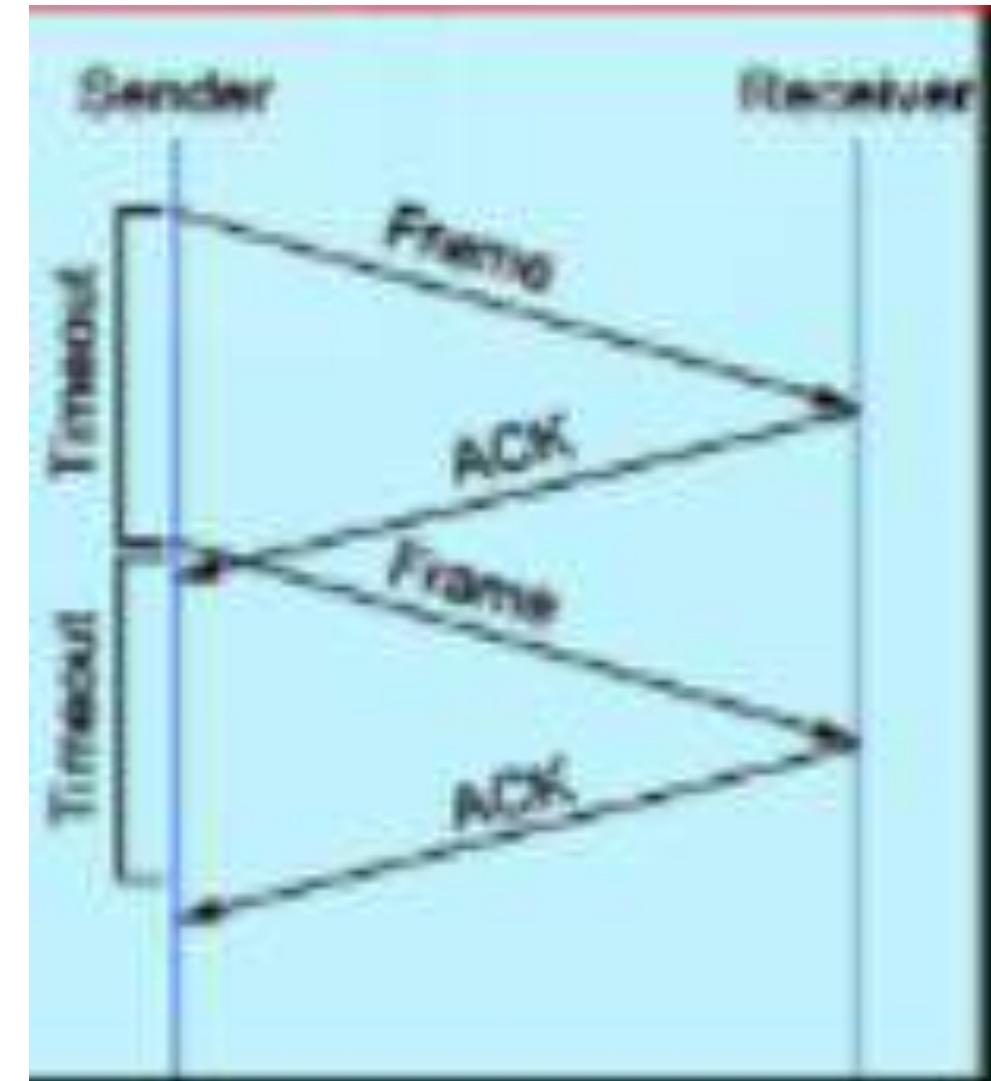
Stop and wait ARQ protocol

ACK is lost



Stop and wait protocol

The timer fires too soon



Sliding window Protocol

- *Go-back-N ARQ*
- *Selective Repeat Request*

The disadvantages of stop-and -wait ARQ protocol is

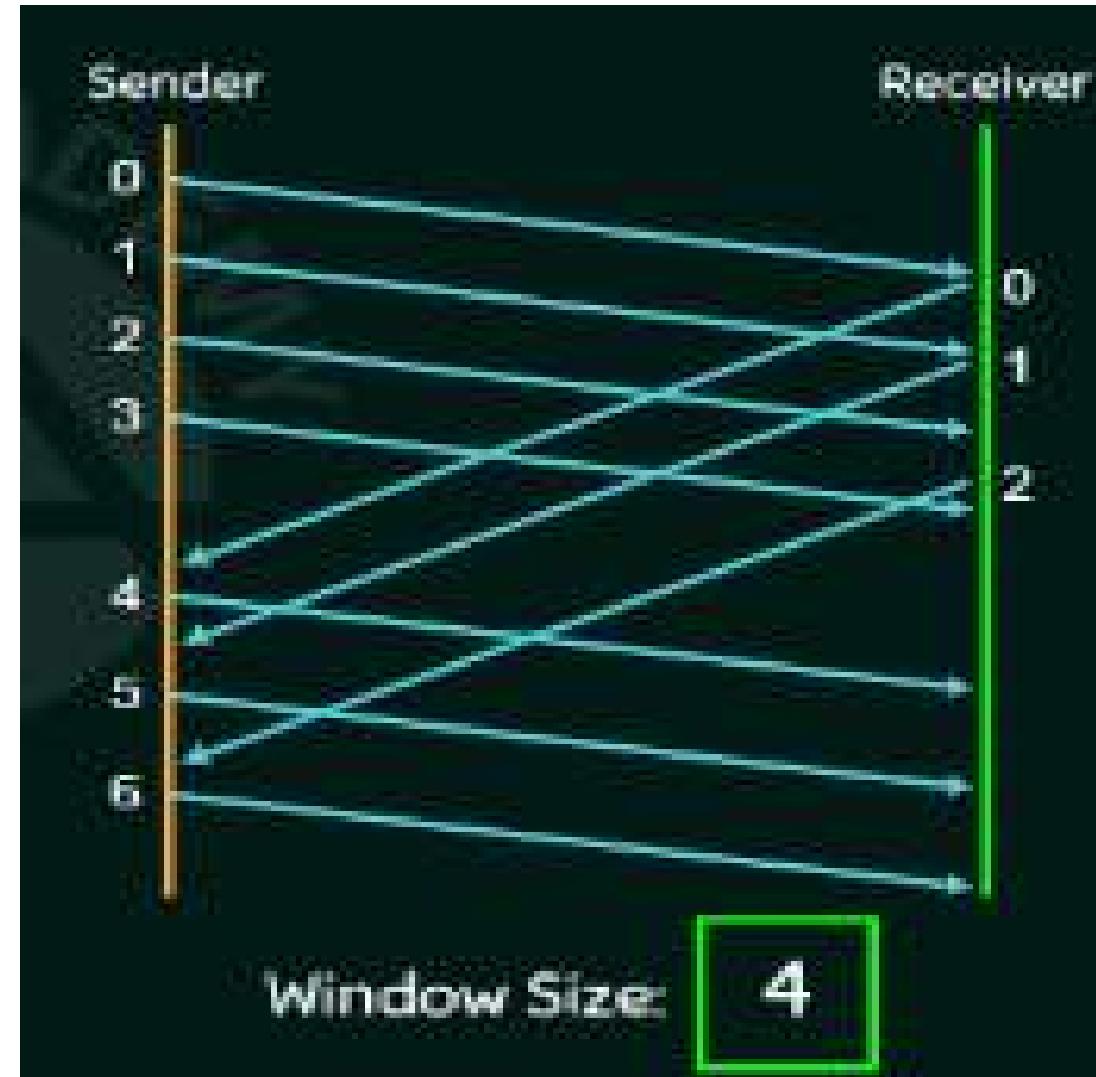
- One frame at a time*
- Poor utilization of bandwidth*
- Poor performance*

The advantages of sliding window protocol is

- Send multiples frames at a time*
- Number of frames to be send is based on the window size*
- Each frame is numbers i.e. each frame is associated with a sequence number.*

Working of sliding window protocol

- Supposes sender has 11 no. of frames to transmit.
- Here 0 to 10 depicts the sequence nos. of the frames.
- Window size of the sender $N = 4$.
- Step 1: Sender will send first four frames at ones.
- Step 2: After getting the ACK from the 0th frame, the window will slide by one position on the left side. And the sender now transmits the 4th frame. Similarly after getting the acknowledgement from the 2nd frame the window slides on the left by one position
- So, there are three categories of frames in the buffer, 0 to 2nd are frames which are sent and got acknowledged, 3 to 6th frame are sent and waiting for acknowledgement, and 7 to 10th frame are not yet sent and in the queue.



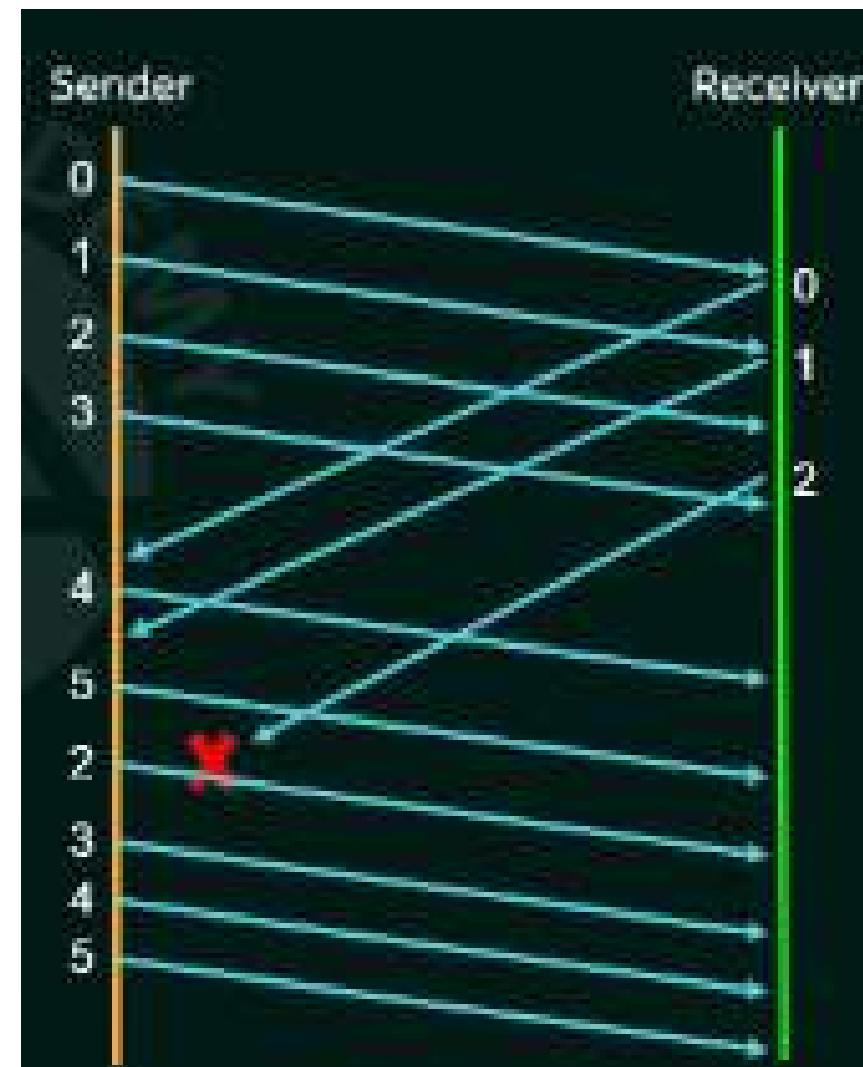
Go-Back-N ARQ protocol

- Here N represents the window size, suppose $N = 4$.
- Supposes sender has 11 no. of frames to transmit.
- Here sequence nos. of the frames depends on the window size

$$N = 4 = 2^2$$

Then the sequence nos. will be 0,1,2,3. (This power represents the number of binary bits required to represents the sequence nos. in its decimal equivalent). The max sequence no. can go up to $\{0,1,2 \dots 2^n - 1\}$.

- In Go-Back-N ARQ protocol the sender can send multiple frames before receiving acknowledgement from the first frame.
- The nos. of frames can be sent depends on the window size.
- If the ACK frames is not received within an agreed period of time, all frames in the current window is retransmitted

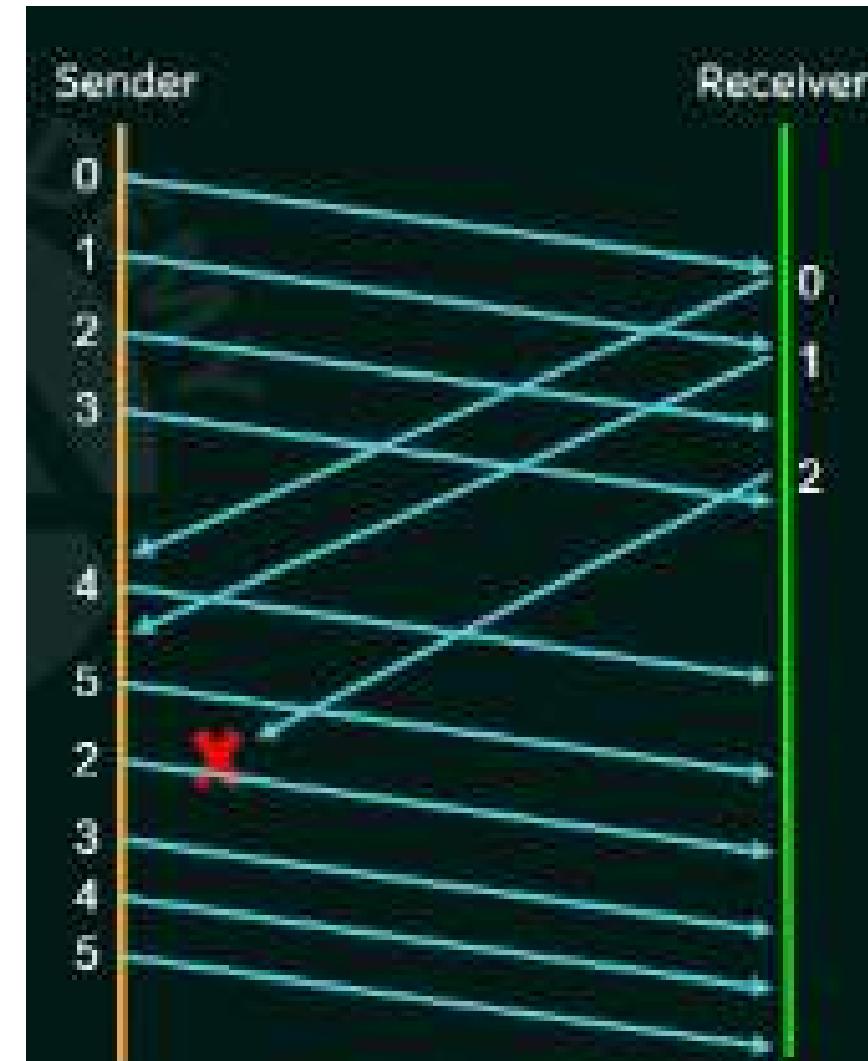


Go-Back-N ARQ protocol

- Supposes sender has sent 4 frames at ones 0,1,2, 3 and also got acknowledgment for the 0th frame.
- Now the window is holding 1, 2,3 and 4th frames. And the sender also got acknowledgment for the frame with sequence no. 1. Now the window of size 4 is containing frames 2, 3, 4 and 5.
- If the acknowledgement from the frame with sequence no.2 is not received then within a finite period of time. Then the sender times out again will transmit all the frames in the window starting from the frame with sequence no. 2. (i.e. 2,3,4,5) again.
- That's why it is called Go-Back ARQ protocol, because if one frame in the window is not acknowledged then the all the frame in the window will be retransmitted again.



Go back to 2

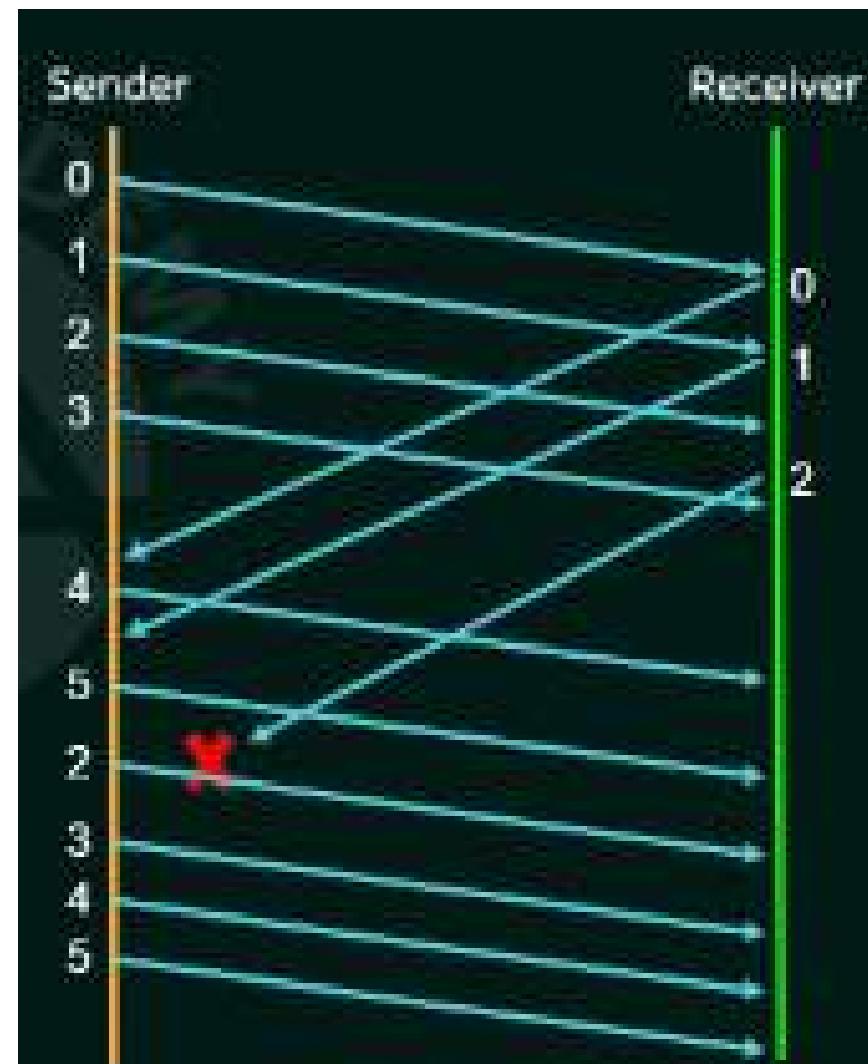


Go-Back-N ARQ protocol

- Sender window size = $N = (1+2a)$ for
- Receiver window size = 1
- Efficiency = $\frac{N \text{ (window size of sender)}}{1+2a}$
- Where $a = \frac{\text{Propagation delay } T_p}{\text{Transmission delay } T_t}$
- Maximum data rate possible/Throughput = Efficiency \times Bandwidth
- Round Trip Time (RTT) = $2 \times T_p$
- Optimal Sender window size = $N = (1+2a)$ for 100% efficiency



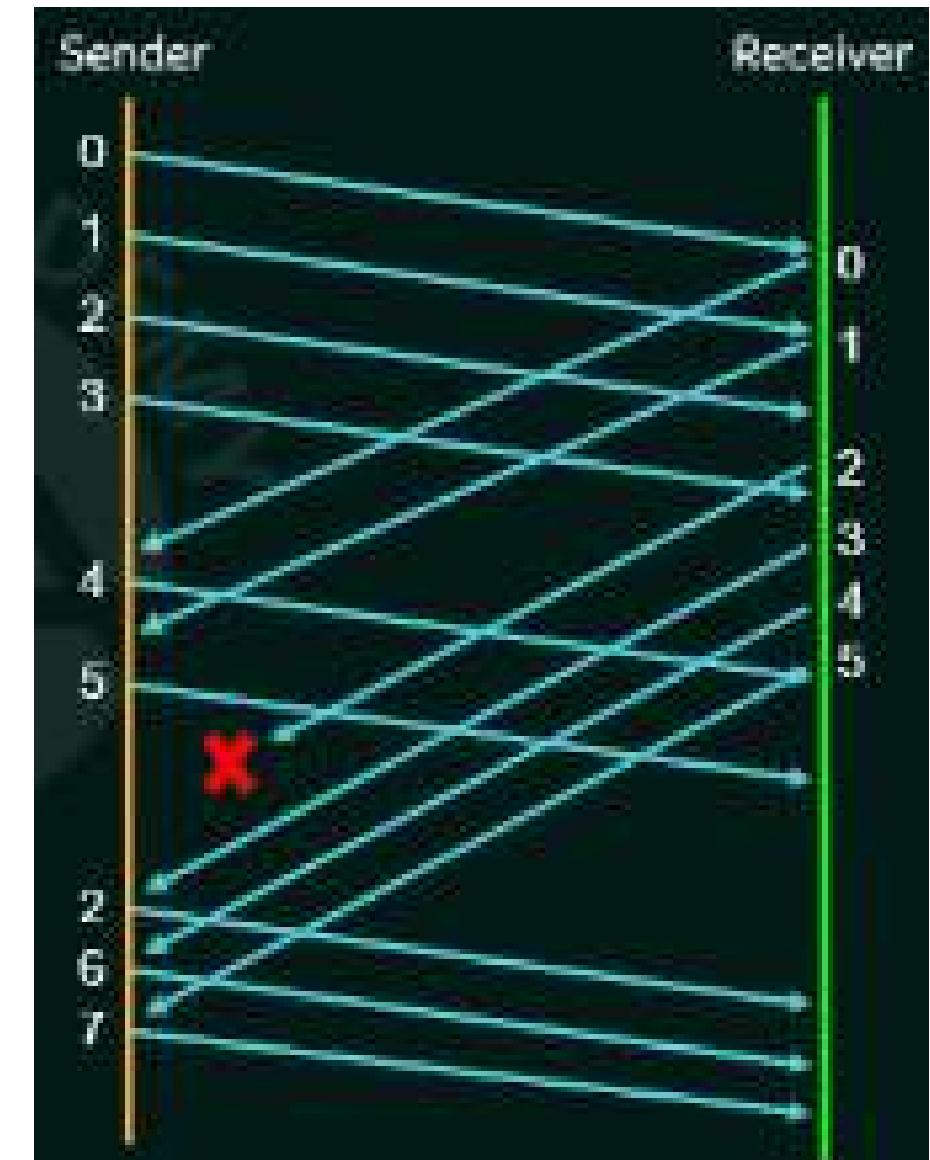
Go back to 2



Selective Repeat Request ARQ Protocol

- In selective repeat ARQ, only the erroneous or lost frames are retransmitted, while correct frames are received and buffered at the receiver side.
 - The receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK (Not Acknowledged) for only frame which is missing or damaged.
 - The sender will send/retransmits the frame for which NACK is received.
 - In this protocol only the required frame is retransmitted and not the entire window.
-
- Sender window size = N
 - Receiver window size = N

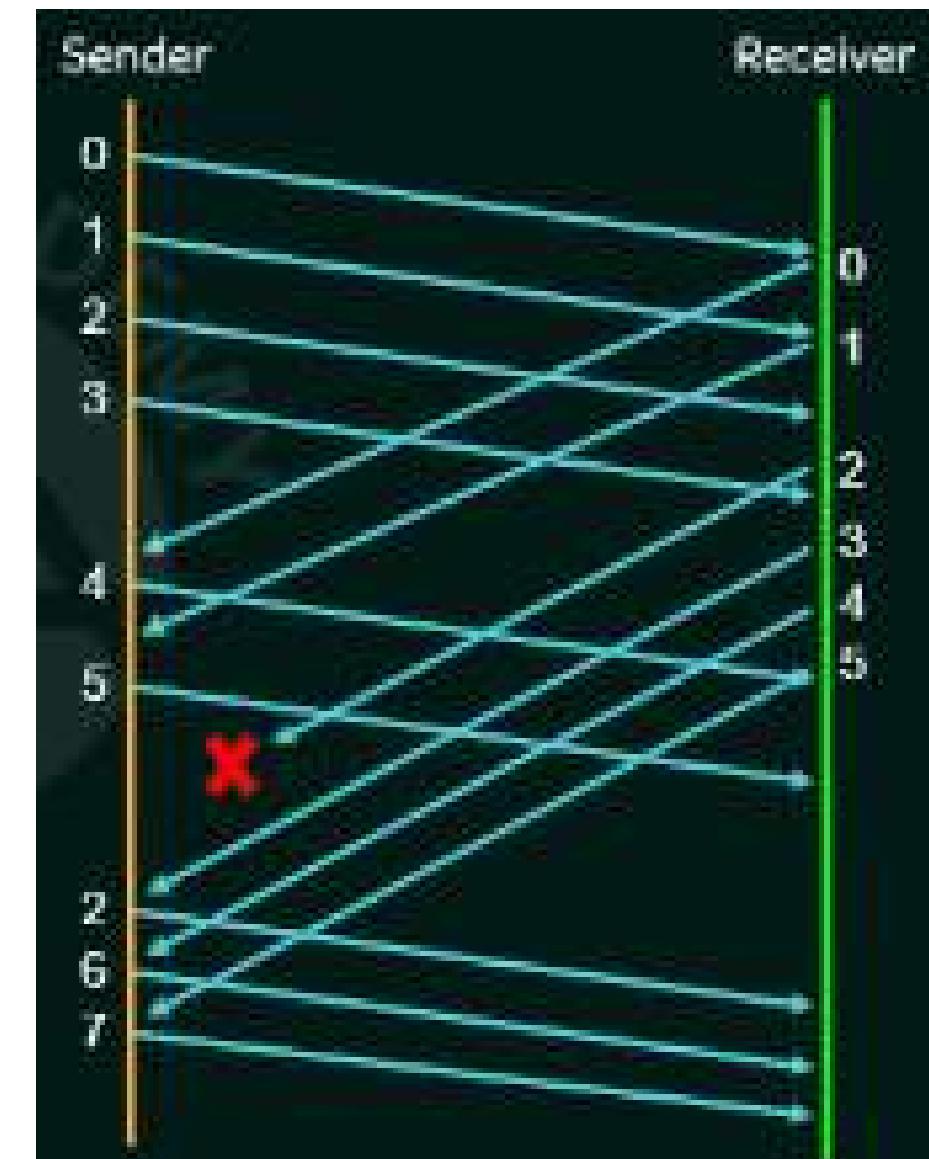
Window Size = 4



Selective Repeat Request ARQ Protocol

- In selective repeat ARQ, only the erroneous or lost frames are retransmitted, while correct frames are received and buffered at the receiver side.
 - The receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK (Not Acknowledged) for only frame which is missing or damaged.
 - The sender will send/retransmits the frame for which NACK is received.
 - In this protocol only the required frame is retransmitted and not the entire window.
-
- Sender window size = N
 - Receiver window size = N

Window Size = 4



5	4	3	2	1	0
---	---	---	---	---	---

window
size = 2

step 1 = sender will transmit Frame
with seq no 0, 1.

5	4	3	2	1	0
---	---	---	---	---	---

after 8th ACK
from the
0th frame

step 2 = Frame seq no 2 will be transmitted

5	4	3	2	1	0
---	---	---	---	---	---

Go-back-N ARQ protocol:-

Sender window size = N^w .

Receiver window size = 1^w

$N = 2^{\text{no. of bits}}$

3-bit sequence number
or
3-bit sequence number
represent the sequence
now.

G10-back-4 ARO

→ Receiver size = $\frac{1}{\sqrt{2}}$ ✓ ✓ ✓

:- ACK for 2, window

contents 3, 4, 5, 6 -
will be transmitted

Box of Transcribed

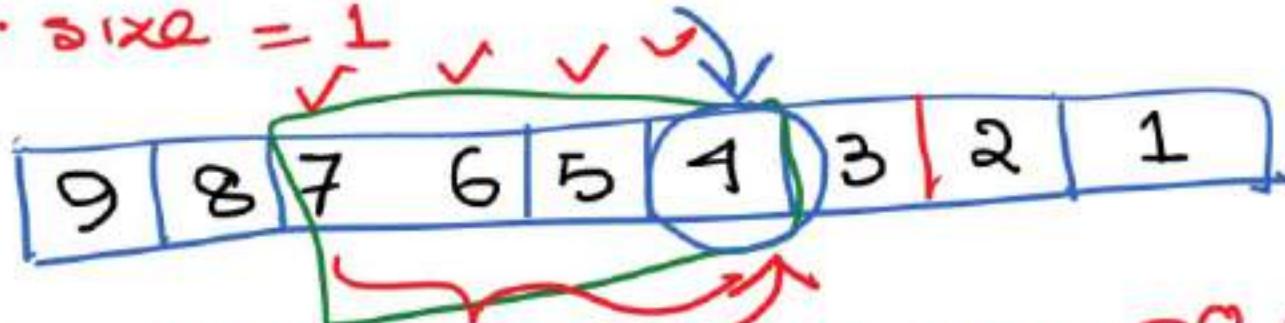
$$\text{frame upon } 11 \text{ now} = 5^{\frac{1}{4}} + 1 = 6$$

- ACK for B, content of

4, 5, 6, 7, now 7

1 be transon if

$$\text{Total no. of found } cG+1 \\ = 7$$



Step 1:- Frame will seq no,
1, 2, 3, A is transmitted.

Total no. of frames transmitted
until now =

Step 2 :- ACK P_0 or Frame seq. no
vs received, now

Windows Context 2, 3, 4, 5

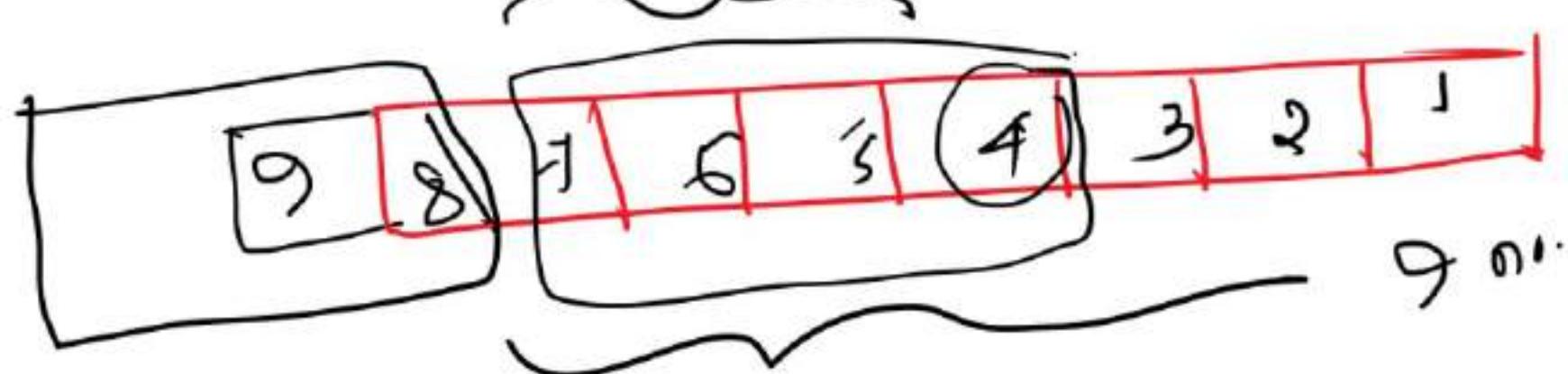
Total no. of frames known
will now = 4+1

4th frame is in error

Step 5:- 4th Frame all the frames in the window will be retransmitted again

Total no. of frame have to be transmit

$$A = 4 + 7 = 11 \text{ w} \\ \underline{\quad\quad\quad}$$



$$11 + 2 \\ \circlearrowleft 13$$

Go-back-N ARQ (Receiver window
size = 1)
* window size = N (sender)

stop-and-wait / stop-and-wait ARQ
window size = 1

↳ window size

Go-back-N ARQ

Go-back-8 ARQ: scoder window
size N = 8

$$N = 2^m$$

3 bit representation

$$N = 2^3 = 8$$

00 → 000
01 → 001
10 → 100
11 → 110

2 bit representation

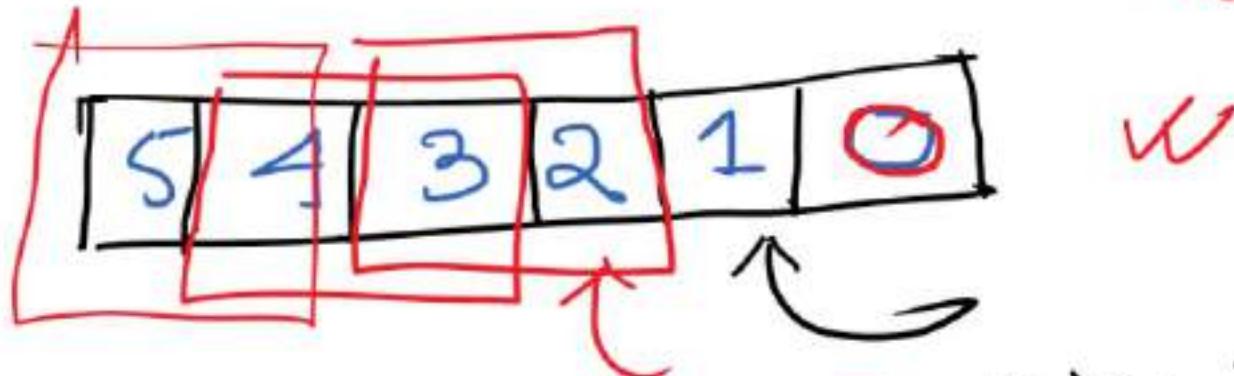
$$N = 2^2 = 4$$

000

111

Sender :- message = 6 Frames

window = 2 ^w

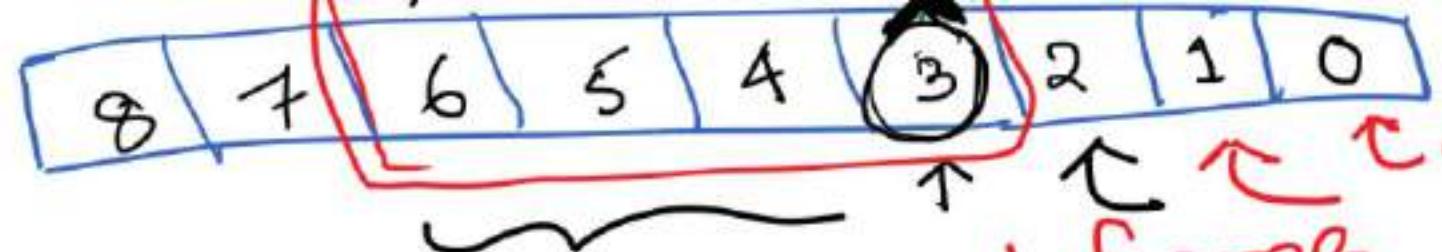


Step 3: - ACK Frame seq. No. 1 , 3 will be

Step 2: - receive send ACK Frame
no. Frame seq. no. 2
will be transmitted

Q: If Frame \Rightarrow window size $\Rightarrow 4$, then the
① 4th frame in the queue has not got ACK and
ACK (4th frame) in the queue is in error.
Now to successfully transmit my
other msg (9 no. Frame) how many no
of frame we have to transmit?

$$* \omega = A = 2$$



#S1:- at a time we can transmit frame with seq. No. 0, 1, 2, 3.

Total no. of frames sent until now = A

#S2:- Frame seq. no. 0 got ACK, frame with sequence no. A vs transmitted now = $(A + 1)$

Total no. of frame sent until now = B

#S3:- Frame seq. no. 1 ACK, seq. no. B will be transmitted

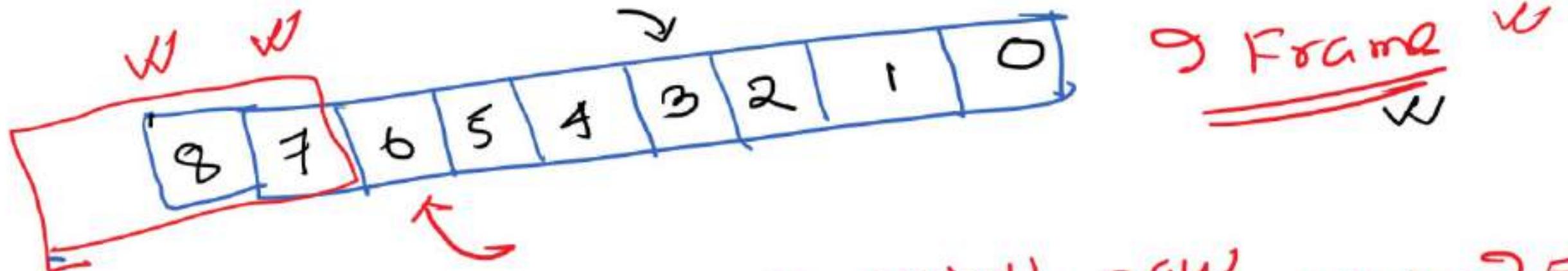
Total no. of frame sent until now = $B + 1 = C$

#S4:- Frame seq. no. 2 ACK, seq. no. C will be transmitted

Total no. of frames sent until now = D

#S5, again we have to transmit frame
with seq no. 3, 4, 5, 6

Total no. of frames sent until now = $7 + 4 = \boxed{11}$



Total no. of frame sent until now = $11 + 2 =$

The queue is
empty

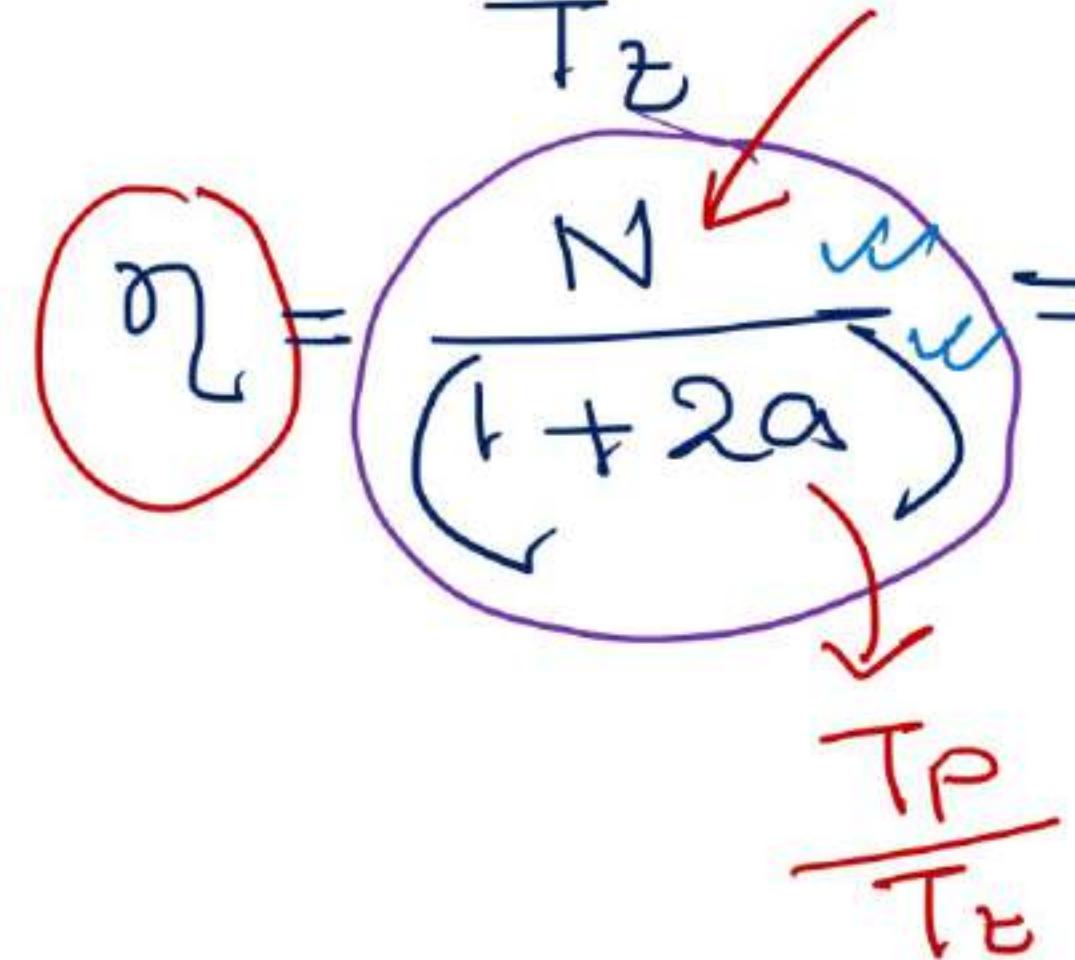
w
Go-back-N ARQ
 sender size w = N
 receiver window size = 1 Selective Repeat ARQ

Efficiency of

Go-back-N ARQ

$$\eta = \frac{N}{(1+2a)} = \dots \times 100\% \quad \begin{matrix} \text{Received} \\ \text{window size} \\ = N \end{matrix}$$

$$a = \frac{T_p}{T_e} \quad \text{windage}$$



$$\begin{aligned} a &= \frac{T_p}{T_e} \\ &= \frac{1 \times 100\%}{w} \\ &= \frac{100\%}{w} \\ N &= (1+2a)w \end{aligned}$$

100

seconds

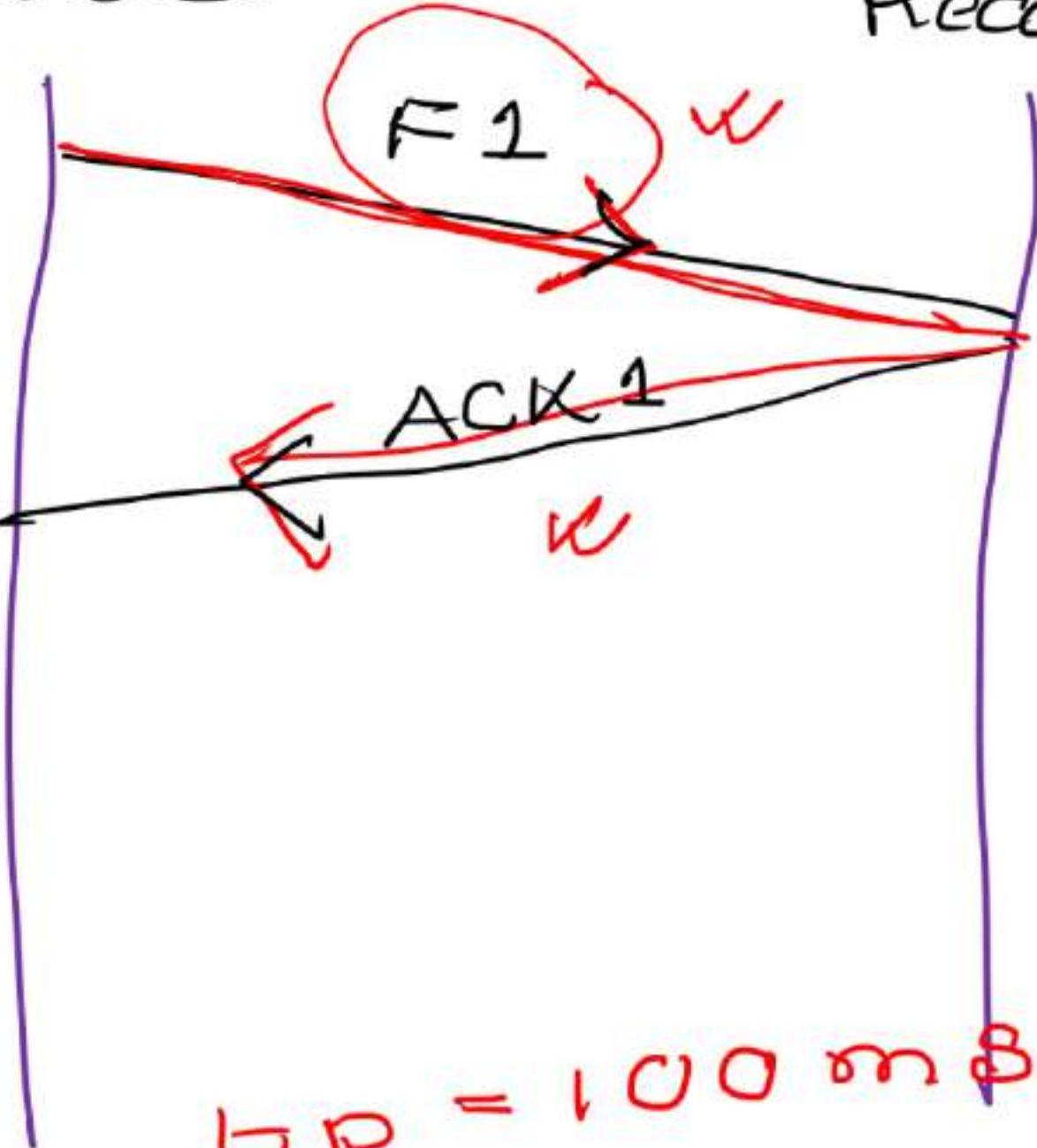
Received

one-way

$$= \frac{100 \text{ Km}}{\text{Speed of light}}$$

$$= \frac{100 \text{ Km}}{1000 \text{ Km/s}}$$

$$= 0.1 \text{ s}$$



$$t_p = 100 \text{ ms}$$

Round-trip

Q. A 20 kbps satellite link has a propagation delay of 400 ms. The transmitter employs a Go-back-N ARQ protocol. $N = 10$. The each frame is 100 bytes long. what will be the max data rate possible?

Max data rate/Throughput

$$= \text{BW} \times \text{efficiency } \eta = \frac{1}{(1+2\alpha)}$$

$$= 20 \text{ kbps} \times \eta$$

$$= 20 \text{ kbps} \times 0.47 = 9.5 \text{ kbps}$$

$$\alpha = \frac{T_P}{T_B}$$

$$\alpha = \frac{1 \text{ ms}}{400 \text{ ms}}$$

Given data :-

service window size $N = 10$

$$\text{Frame} = 100 \text{ bytes} \\ = 100 \times 8 \text{ b}$$

$$T_P = 400 \text{ ms}$$

$$\text{BW (Transmission)} = 20 \text{ kbps}$$

$$T_P = \underline{\underline{400 \text{ ms}}},$$

$$T_t = \frac{\text{Packet size (in bits)}}{\text{Transmission rate / B}}$$

$$\alpha = \frac{T_P}{T_2} = \frac{400 \cancel{\text{ms}}}{40 \cancel{\text{ms}}} = 10^4$$

$$\eta = \frac{N^w}{(1+2\alpha)}$$

$$= \frac{10}{(1+2 \times 10)} = \frac{10}{21} = 0.47^w$$

$$= 47\%.$$

$$= \frac{100 \text{ bytes}}{20 \text{ kbps}} = \frac{100 \times 8 \text{ bits}}{20 \times 10^3 \text{ bits/s}}$$

$$= 40 \times 10^{-3} \text{ s}$$

$$T_2 = 40 \text{ ms} \text{ } w.$$

Q. Message sender size each frame 5000 bits of data, Total msg size 1 Million (10^6 bits)

- a. Stop-and-wait ARQ
- b. Go-back-N ARQ
- c. Selective Repeat ARQ

How long all these ARQs will take send the entire msg.

* No Data & ACK is lost in

All these ARQs are using 3 bits for retransmission
Sq. No. → If the sender & receiver bytes sender & receiver
5000 km & propagation speed 2×10^8 m/s

Ignore Transmission & processing delay
waiting & queueing delay

Given Data:- Frame size = 5000 bits.
 Message size = 10^6 bits
 RTT delay : Distance bet Scodes & Recvers = $5000 \times$
 and Trip Time delay : Propagation speed = $2 \times 10^8 \text{ m/s}$
 : 1 no. of frames
 = $\frac{10^6 \text{ bits}}{5000 \text{ bits}}$
 = $\frac{1000 \times 10^3}{5 \times 10^3}$ = 200 Frames
 = $\frac{5 \times 10^6}{2 \times 10^8} \text{ s} = 2.5 \times 10^{-2} \text{ s}$

$$RTT \left(\text{Scal the Frame} + \text{Scal the ACK} \right) = 25 \text{ ms} + 25 \text{ ms} = 50 \text{ ms}$$

stop-and-wait ARQ = $\frac{50 \text{ ms}}{200} = 10 \times 10 = 10$

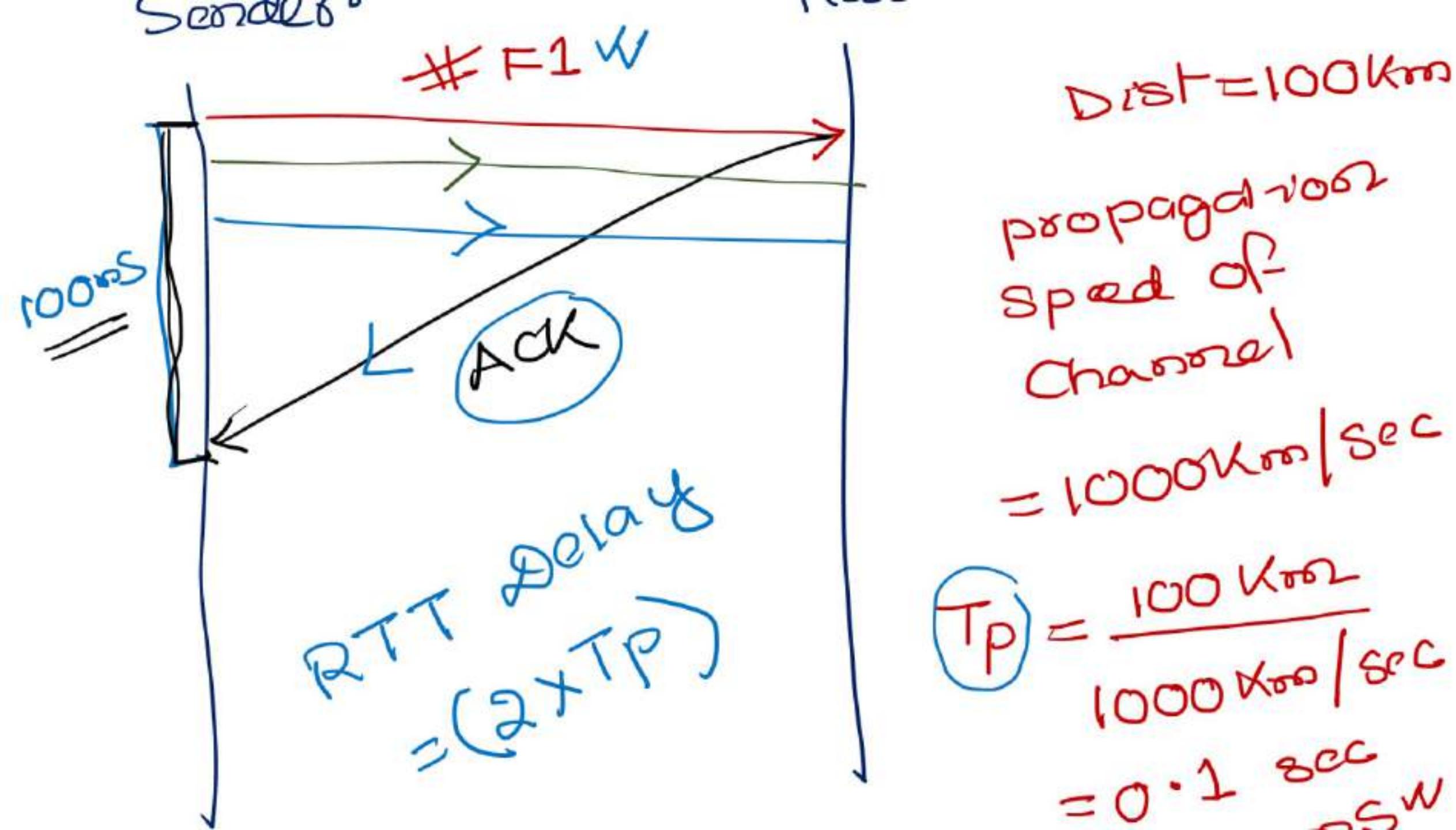
↓ window
 Go-back-N ARQ = $\frac{200}{8} \times 50 \text{ ms} = 125$

⇒ Selective-repeat ARQ = $\frac{200}{8} \times 50 \text{ ms} = 1250$

* Disadvantage of Go-back-N ARQ

→ if a frame is in error &
didn't get acknowledgement
then the entire window has to
be transmitted again

→ waste



$$Dist = 100 \text{ km}$$

propagation
 speed of
 channel

$$= 1000 \text{ km/sec}$$

$$TP = \frac{100 \text{ km}}{1000 \text{ km/sec}}$$

$$= 0.1 \text{ sec}$$

$$T_t = \frac{\text{Packet size (bits)}}{\text{Transmission rate / BW of the link}}$$

Go-back-N ARQ

$\eta = \frac{N}{(1+2\alpha)^w} = N$

$\eta = 100 \Rightarrow N = 100$

$\alpha = \frac{TP}{Tr} = 1$

$\frac{N}{2\alpha} < 1$

second window size = N^w

received window size = 1

$$\eta = \frac{N}{(1+2\alpha)}$$

To achieve 100 % efficiency
will be optional window size

$$\frac{N}{(1+2\alpha)} = 1$$
$$N = (1+2\alpha)$$

↑
optional window size

$N = 2^{m/2}$
 $m = 60$. of bits
for processor

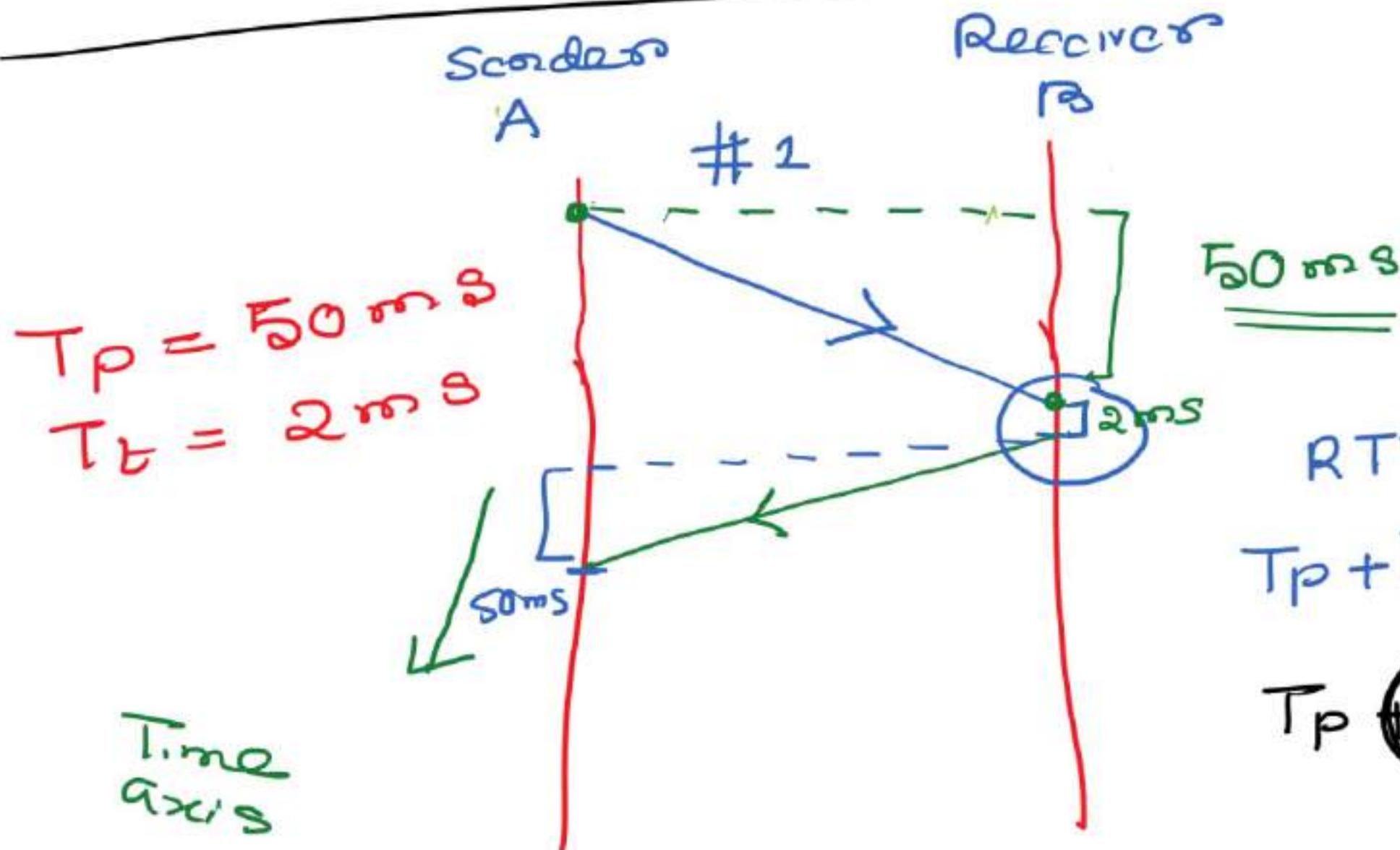
3-bit representation

$$N = 2^3 = 8$$

$\{0, 1, \dots, 2^m - 1\}$

↑
ord-seqno.

*Selective Repeat request ARQ



Total
IP
RTT

Q. A 20 kbps satellite link has a propagation delay of 400 ms. The transmitter employs a 'Go-back-N ARQ' $N = 10$. Assuming that each frame is 100 bytes what is the maximum data rate possible?

* maximum data rate possible / Throughput

= Efficiency \times Bandwidth.

$$\eta \times 20 \text{ kbps}$$

$$\frac{\eta}{N} \times \frac{20 \text{ kbps}}{(1+2\alpha)}$$

$$T_B = 40 \text{ ms}$$

$$T_B = \frac{\text{Packet size (bytes)}}{\text{Transmission rate (BW)}}$$

$$= \frac{100 \times 8}{20 \times 10^3}$$

Given Data

BW = 20 kbps

$T_p = 400 \text{ ms}$

$N = 10$ (window size)

$$a = \frac{T_P}{T_E} = \frac{400 \text{ ms}}{40 \text{ ms}} = 10^w.$$

↗

$$\frac{10}{(1+2 \times 10)} = \frac{10}{21}$$

$$= 0.47$$

$$= 47\%$$

Max. data rate possible

$$= \pi \times \beta \omega$$

$$= 0.47 \times 20 \text{ kbps}$$

$$= \frac{9.4 \text{ kbps}}{\approx 10 \text{ kbps}}$$

- Q. each frame carries 5000 bits of data,
how long it takes to send 1 million bits of data
a. stop-and-wait ARQ. b. Go-back-N ARQ
c. selective repeat ARQ.

Assume that all these three ARQ are using 3 bit
representation for seq-No. The distance between the
sender & receiver 5000 km and propagation
speed 2×10^8 m/s. Assuming no frame or ACK
& also assume there is no transmission delay
waiting & processing delay -

Given Data :- Frame size = 5000 bits
 dist = 5000 km
 propagation speed = 2×10^8 m/s

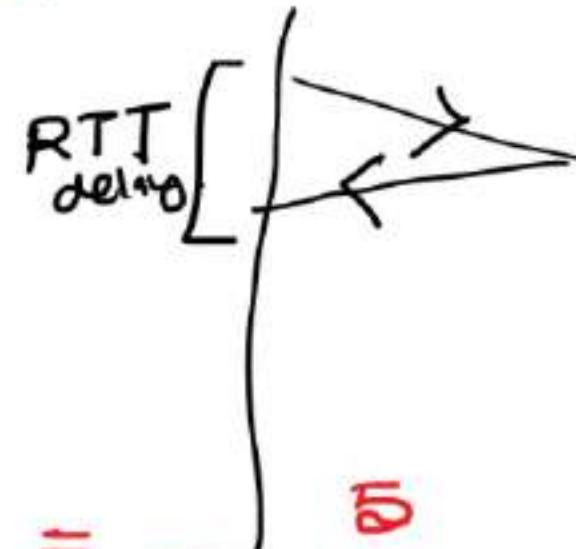
Total no. Frames

$$= \frac{10^6 \text{ bits}}{5000 \text{ bits}}$$

$$= \frac{10 \times 10^5}{5 \times 10^3} = 200 \text{ Frames}$$

Total size of data = $\frac{10^6}{2^3} = 8$ bits

$$\text{window size} = 2^3 = 8$$



$$T_P = \frac{\text{distance}}{\text{propagation Speed}} = \frac{5000 \text{ km}}{2 \times 10^8 \text{ m/s}}$$

$$= \frac{5 \times 10^6}{2 \times 10^8} = 2.5 \times 10^{-2} \text{ sec}$$

$$\text{RTT delay} = 2 \times T_p = 2 \times 25 \text{ ms} = \boxed{50 \text{ ms}}$$

* Stop-and-wait ARQ = (sender = receiver = 1)
 Since only one frame can be transmitted window size
 $= 50 \text{ ms} \times 200 = 10,000 \text{ ms}$

→ Go-back-N ARQ = ~~$50 \text{ ms} \times \frac{200 \text{ Frame}}{8 \text{ ms}} = 1250 \text{ ms}$~~

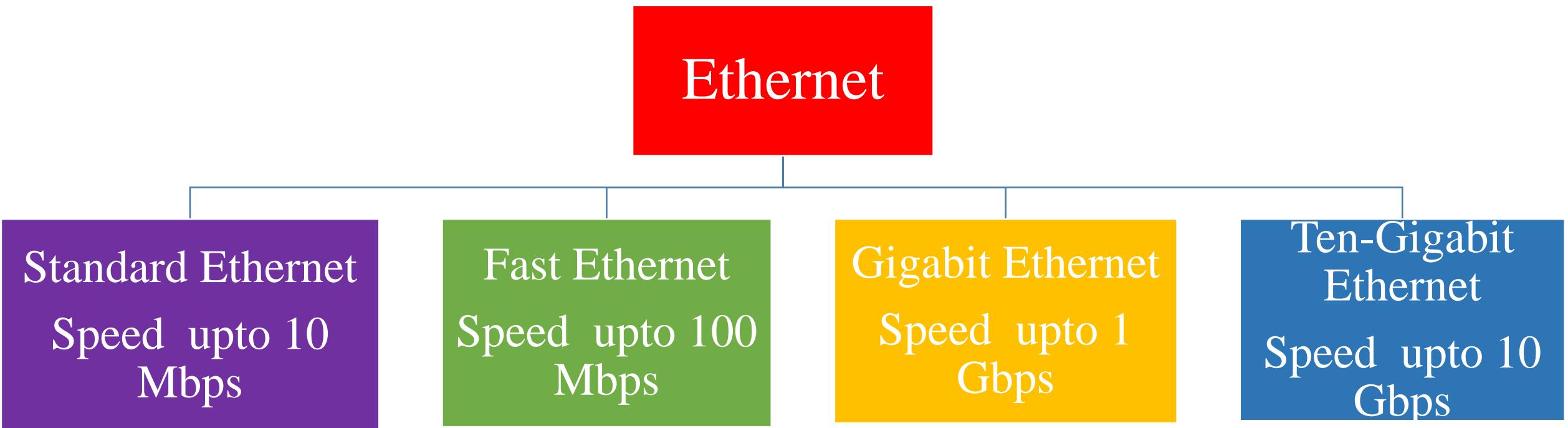
- No error in trans / ACK

→ Selective Repeat ARQ = $50 \text{ ms} \times \frac{200}{8} = 1250 \text{ ms}$

Ethernet

- *Ethernet is the most widely used wired LAN technologies.*
- *Ethernet protocol operates in data link layer and physical layer.*
- *Ethernet is in the family of networking technologies that are IEEE 802.2 and 802.3.*
- *Supports data bandwidth of 10 Mbps, 100 Mbps, 1000 Mbps, 40, 000 Mbps and 1 Gbps.*
- *In this protocol only the required frame is retransmitted and not the entire window.*
- *Ethernet standards define Layer 2 protocol and Layer 1 technologies.*
- *Ethernet operates in two separate sublayer of data link layer logical link layer and MAC sublayer.*

Evolution of Ethernet

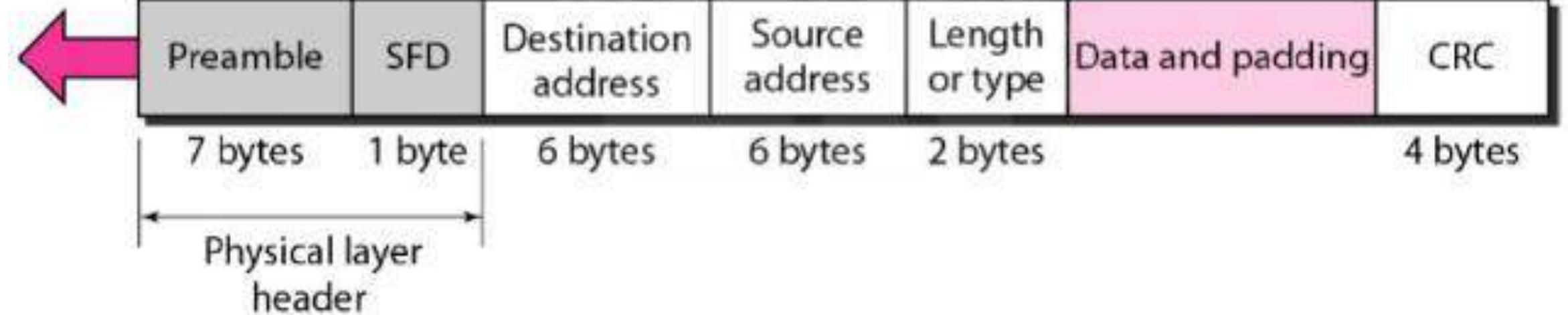


Ethernet Frame Format

- *Preamble: 56 bits of alternating ‘1’s and ‘0’s. It is needed for synchronization purpose.*
- *SFD (Start Frame Delimiter): Flag 10101011. This also needed for synchronization purpose. The last two bits of the Flag indicates the next field of the Ethernet frame is the destination address.*
- *Padding is required to make the received data from the upper layer (i.e network layer) a fixed size length.*

Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)

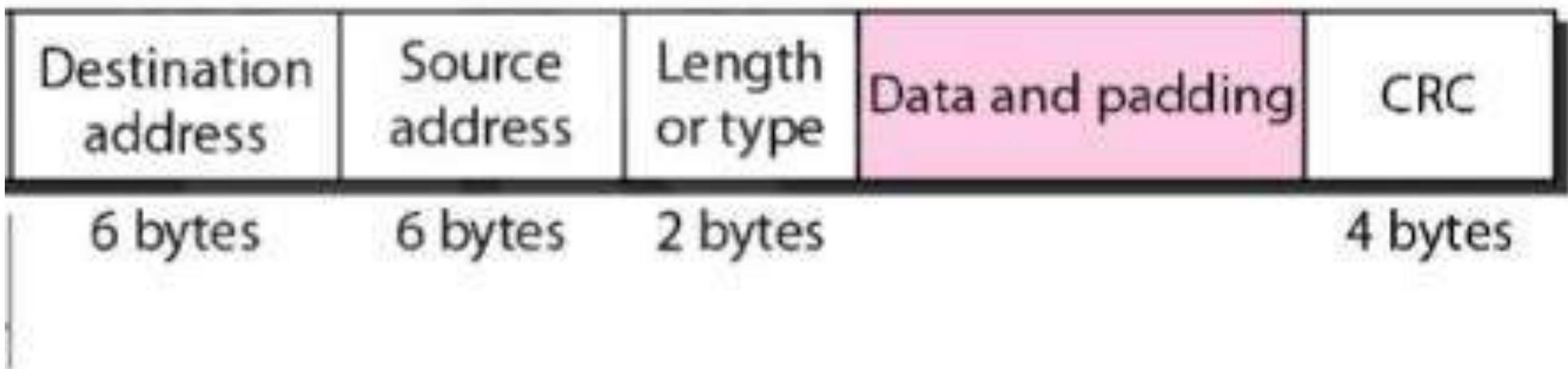


Minimum and Maximum Length of the Ethernet Frame

Payload from the network layer

Min payload = 46 bytes

Max. payload = 1500 bytes



Min size of the Ethernet frame = 64bytes

Max. size of the Ethernet frame = 1518bytes

Ethernet Address

Example: **06:01:02:01:2C:4B**



- *The least significant bit of the first byte defines the type of the address*
- *Last bit 0 defines Unicast, otherwise multicast*
- *If all bits in the frame is ‘1’ then this is Broadcast.*

Module 3

Network Layer



Dr. Sunandita Debnath, IIIT Vadodara

IPV4 Address

- *IPV4 addresses are 32 bits long that uniquely and universally defines the connection of a device on the internet.*
- *IPV6 addresses are 128 bits long.*
- *Two devices on the internet can never have the same addresses at the same time.*
- *The addresses range of IPV4 addresses are 2^{32} i.e. more than 4 billions*
- *But we have more devices, the NAT (network address translation) technology will resolve this.*

IPV4 Address

- *IPV4 addresses have two notations*
 - *Binary notations.*
 - *Dotted Decimal notations.*

Binary notations: 01110101 10010101 00011101 00000010

Dotted Decimal notations: 117.149.29.2

- *IPV4 addresses consist of four octets each octet consists of 8 binary bits.*
- *Each octet ranges from 0 to $2^8 - 1 = 255$*

IPV4 Address Conversion

- Binary to Dotted Decimal conversion**
- Dotted Decimal to Binary Conversion**

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

Binary Notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–239			
Class E	240–255			

Decimal Notation

Address Class	1st Octet range in decimal	1st Octet bits (Blue Dots do not change)	Network (N) and Host (H) Portion	Default mask (Decimal)	Number of possible networks and hosts per network
A	0-127	00000000 01111111	N.H.H.H	255.0.0.0	128 Nets (2^7) 16,777,214 hosts ($2^{24}-2$)
B	128-191	10000000 - 10111111	N.N.H.H	255.255.0.0	16,384 Nets (2^{14}) 65,534 hosts ($2^{16}-2$)
C	192-223	11000000 - 11011111	N.N.N.H	255.255.255.0	2,09,150 Nets (2^{21}) 254 hosts (2^8-2)
D	224-239	11100000 - 11101111	NA (Multicast)	-	-
E	240-255	11110000 - 11111111	NA (Experimental)	-	-

Subnet Mask (Slash Notation)

Class	Subnet Mask (in Dotted Decimal)	Subnet Mask (in Binary)	Slash Notation
A	255.0.0.0	1111111.0000000.0000000.0000000	/8
B	255.255.0.0	1111111.1111111.0000000.0000000	/16
C	255.255.255.0	1111111.1111111.1111111.0000000	/24

IP address	<p>Network portion of IP address Host portion of IP address</p>  <p>192.168.10.2</p>
Subnet Mask	255.255.255.0

“Ethernet protocol → Data link layer”

“Ethernet technologies → physical layer”

IEEE 802.2 & 802.3

IEEE 802.11

Bluetooth & WiFi

A Ethernet MAC sublayer received 42 bytes from the network layer, how many padding bytes should be required?

→ min payload size = 16 bytes

42 bytes \Rightarrow $16 - 42 \Rightarrow 4$ bytes

Data received from the upper layer 1530 bytes?

Then how the data will be transmitted?

→ max size payload = 1500 bytes

Received data = 1530 bytes

↓
We can't send it in a single

Frame(1) = 1500 boxes

Frame(2) = 30 boxes < 46 boxes

$46 - 30 = 16$ boxes min size
of paylow

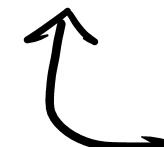
padding m

the Frame 2 v

06:01:02:1:2C:4B \Rightarrow

Address of Ethernet Frame

06 \Rightarrow 0000 0110



LSIB3 = 0 \Rightarrow unicast address

LSIB3 \Rightarrow 1 \Rightarrow multicast

All bits connect to 1 \Rightarrow broad

Hex → decimal → Binary

0	-	---	0	- - - .	8 1 2 1
1	- -	- .	1	0 0 0 0	0 0 0 1
.					
9	- - - - - .	9			
A	- - - - - .	10	- - - - -	10 10	
B	- - - - - .	11			
C	- - - - - .	12			
D	- - - - - .	15		1 1 1 1	

FF : FF : FF : FF : FF : FF
47 : 20 : 1B : 2E : 08 : EE

8121

47 → 0100G111

multicast

47 : 20 : 1 B : RE : 08 : EE

8
0
0
0

how it will send out on the cable?

- address will be sent left to right $B \Rightarrow 11$
- now in byte we will right to left $E - 14$
- binary equivalent $8921 \rightarrow 1248$ format

74 : 02 : B1 : E2 : 80 : EE

1110 0010 0000 0100 1101 1000 0111 0100 0001 0000
0111 01

LAN → wireless LAN (802.11)



↓
bluetooth
WiFi

wired LAN (Ethernet)

802.2 & 802.3

Ethernet cross wire

Ethernet — Layer 1 (physical layer)
Technology

— Layer 2 (Data link layer)
Protocol

Data and Padding \Rightarrow

The data received from the upper layers
(network layer) can be of variable
padding

Min \Rightarrow 46 byte ⁿ

Max \Rightarrow 1500 byte

42 bytes +

$$(46 - 42) = 4 \text{ bytes}$$

Maximum size of Ethernet Frame

$$6+6+2+1500+4=1518 \text{ byte}$$

Minimum size of Ethernet Frame

$$6+6+2+46+4=64 \text{ bytes}$$

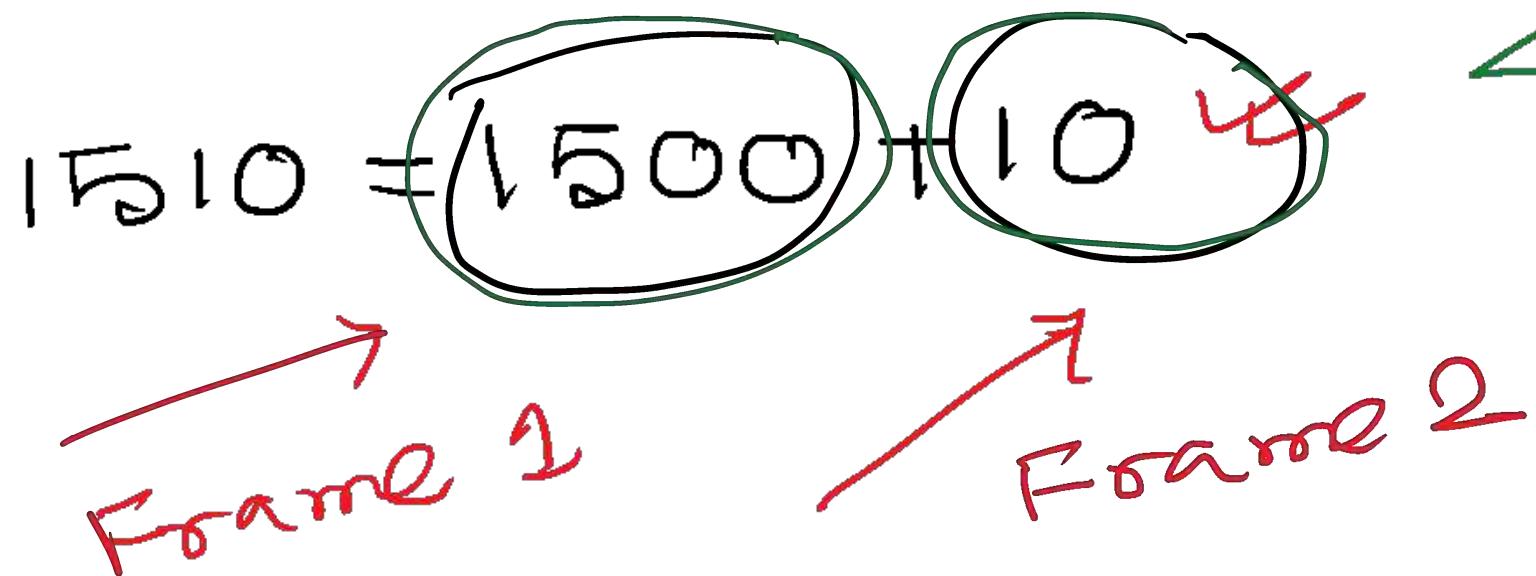
64 bytes 1518 bytes

Q : An Ethernet MAC sublayer receives 1510 bytes of data from the upper layer. Can the data be encapsulated in one single frame? If not how many frame is required? What is the size of each frame?

network layer have size = 1510 bytes

Max = 1500 bytes

Two Frame to send this 1510 bytes



$$\begin{aligned} 1510 &= 1500 + 10 \\ 46 - 10 &= \underline{\underline{36 \text{ bytes}}} \\ &\text{of Padding} \end{aligned}$$

$(5B)_{16} \Rightarrow 5\textcircled{11}$

0101 1011

equivalent

Decimal

0
1
-
9

10

11

Hexadecimal

0
1

9

A

B

Binary

8	4	2	1
0	0	0	0
0	0	0	1
1	0	0	1

Ethernet Frame Address

47:20:1B:2E:08:EE

$$\text{Ethernet} = 48 \text{ bits} = (6 \times 8) \\ = 48 \text{ bytes}$$

0100 0111

LSB

0 \Rightarrow unicast

11111111
1 \Rightarrow multicast

broadcast

u

47:20:1B:2E:08:EE

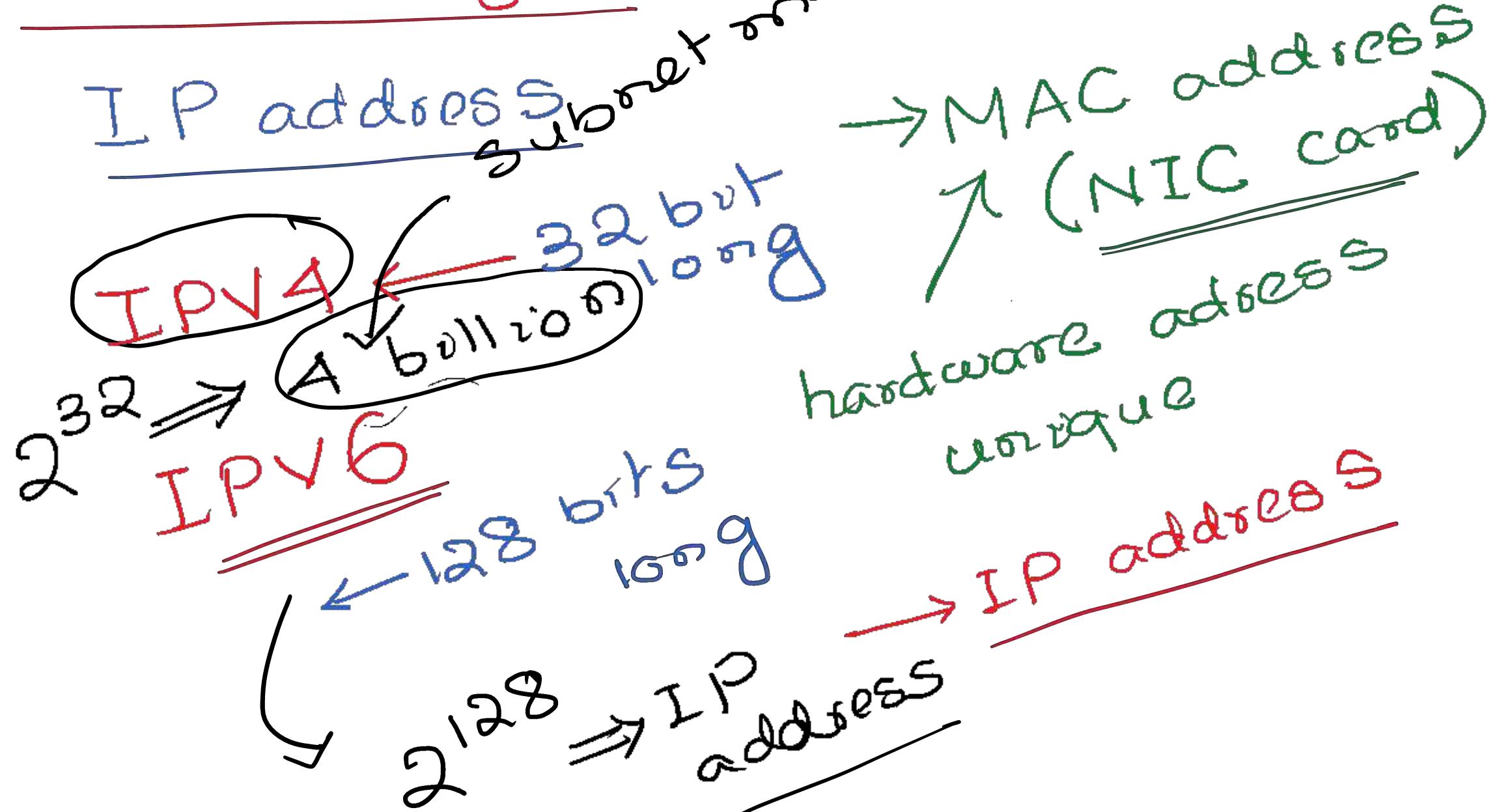
74 02 31 E2 80 EE

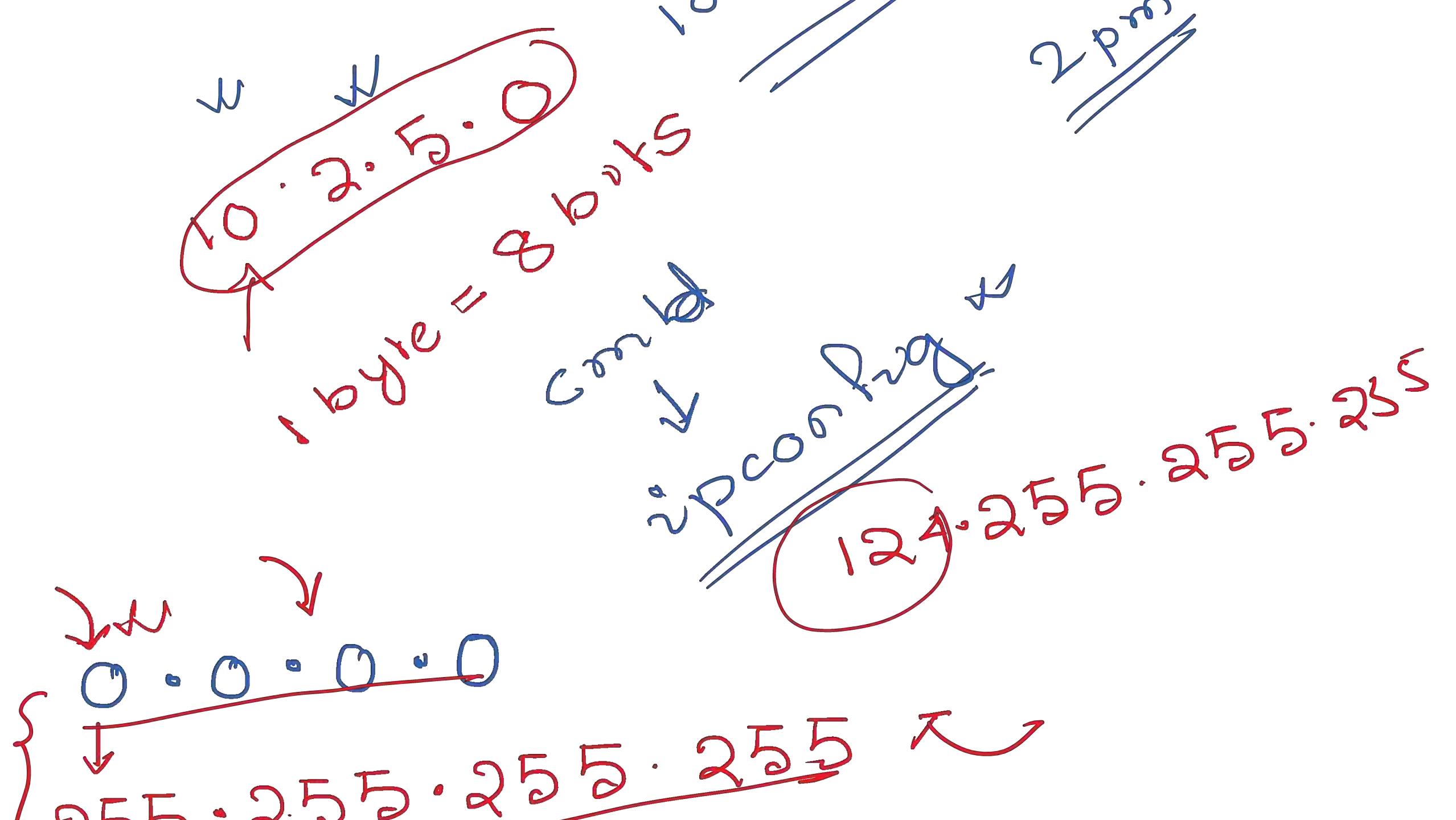
10000010011011000101100000100010111011

net cable (physical)

' ' (0)

Network layers





IPv4 address 0.0.0.0

255.255.255.255

Valid address

99.88.67.89

1.2.3.6

100.200.230.6

Invalid Address (IPv4 \Rightarrow 4 octets)

56.89.1.2.4 \rightarrow 5 octets

232.2.257.0 \rightarrow invalid

$\nwarrow > 255$

10.65.42.98 \rightarrow ^{no prefix}
^{0.1.2.3}
^{zero}
invalid address

IPv4

~~IPV4~~

Binary notation — Decimal notation

$$\begin{array}{ccccccccc} & 2^6 & 2^5 & 2^4 & 2^3 & 2^2 & 2^1 & 2^0 & 2^4 \\ & 32 & 32 & 16 & 8 & 4 & 2 & 1 & 16 \\ 1110 & 1111 & 1111 & 0111 & 11000111 & 000111 & 000011 & 00011 & 11 \\ \underbrace{\hspace{1cm}}_{A} & & & & & & & & \end{array}$$

239 B 247 C 199 D 29

$$0 < A, B, C, D < 255$$

$$128 \cdot 8 \cdot 15 \cdot 1$$

00001000 00001111 00000001

IPv4 \Rightarrow $0 \cdot 0 \cdot 0 \cdot 0$] 2^{32} address
 $255 \cdot 255 \cdot 255 \cdot 255$]
MSB of First byte
First bytes
0 - 127 class A
128 - 191 class B
192 - 223 class C
224 - 239 class D
240 - 255 class E

Class A \Rightarrow $0 \underbrace{00000000}_{\begin{smallmatrix} 6 \\ 2 \\ 2 \\ 2 \\ 2 \\ 2 \\ 2 \\ 0 \end{smallmatrix}} \rightarrow 0$
 $0 \underbrace{11111111}_{\begin{smallmatrix} 7 \\ 2 \\ 2 \\ 2 \\ 2 \\ 2 \\ 2 \\ 1 \end{smallmatrix}} \rightarrow 127$

Class B \Rightarrow $\underbrace{10}_1 \underbrace{0000000}_{\begin{smallmatrix} 6 \\ 2 \\ 2 \\ 2 \\ 2 \\ 2 \\ 2 \\ 0 \end{smallmatrix}} \rightarrow 128$
 $\underbrace{10}_1 \underbrace{111111}_{\begin{smallmatrix} 7 \\ 2 \\ 2 \\ 2 \\ 2 \\ 2 \\ 2 \\ 1 \end{smallmatrix}} \rightarrow 191$

First byte

192 - 223

Class C 110 00000 → 192

110 11111
2⁸ 2^{1 2⁰} → 223

class D

1110 00000] 224

1110 1111] 239

First bytes

224 - 239

total

class E

spose

1111 0000] 240

1111 1111] 255

First bytes

240 - 255

255 - 255 - 255

~~192 · 168 · 2 · 1~~ → class C

~~255 · 255 · 255 · 0~~ →

~~N · N · N · H~~

Host of
address

CLASS A

~~125 · 168 · 2 · 1~~

First bytes Second bytes 3rd 4th = 0

bytes

bytes

3rd

4th = 0

125

0.2.1



0 < 125 < 127

class A → subnet mask

255

0.0.0

N

H H H

1

125

0.2.1

0 - 127

0 bit vs to classify class

0000000] 7 bits

1111111

~~2⁷~~

=

(28)

networks

(6, 177, 214)

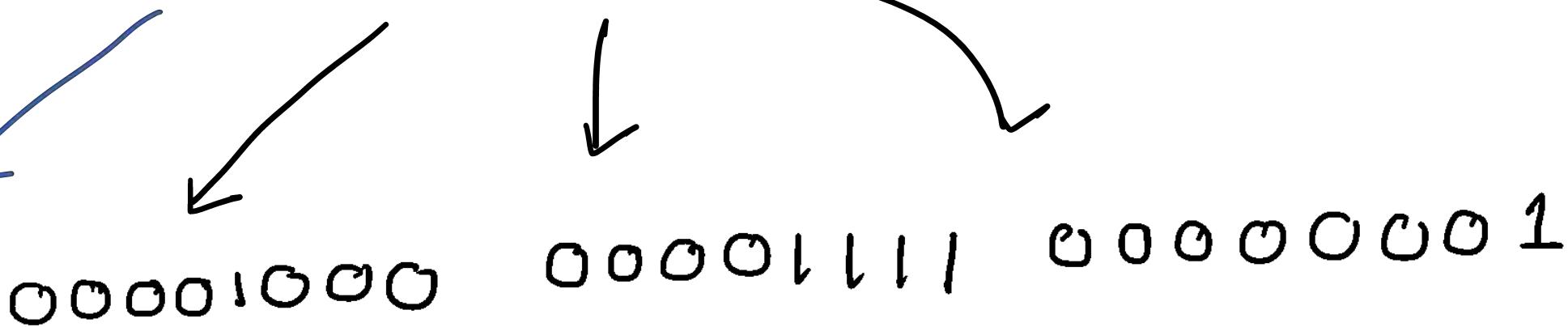
host

2²⁴

~~2²⁴~~

=

$$128 \cdot 8 \cdot 15 \cdot 1$$



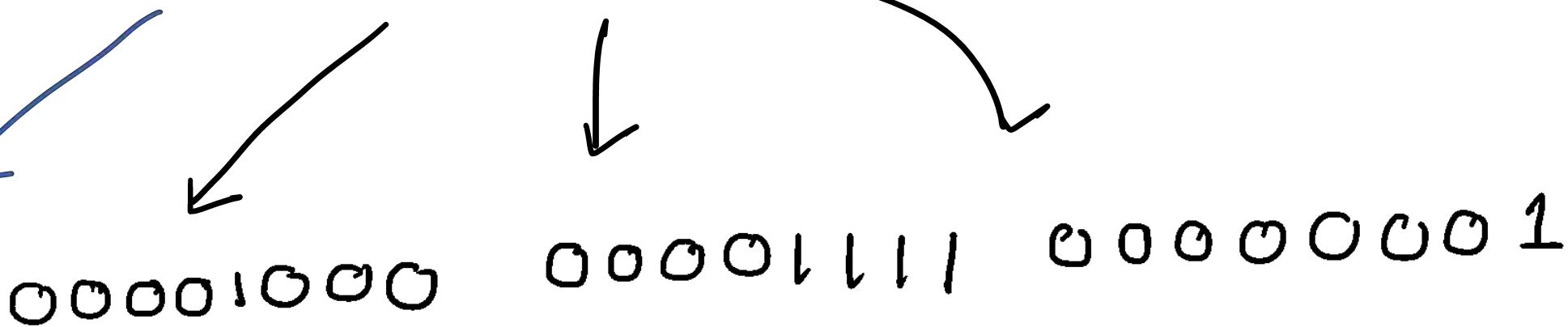
$$128 \cdot 8 \cdot 15 \cdot 1$$

00001000 00001111 00000001

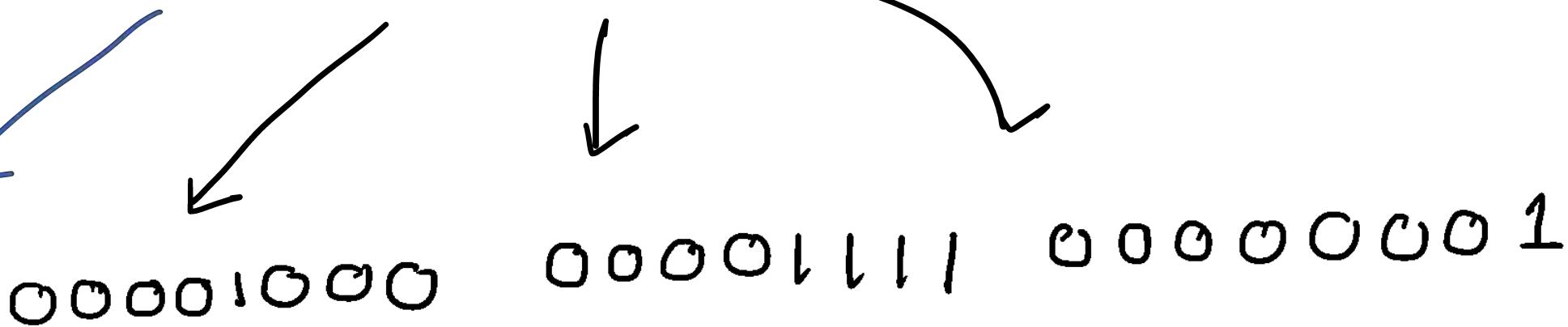
$$128 \cdot 8 \cdot 15 \cdot 1$$

00001000 00001111 00000001

$$128 \cdot 8 \cdot 15 \cdot 1$$



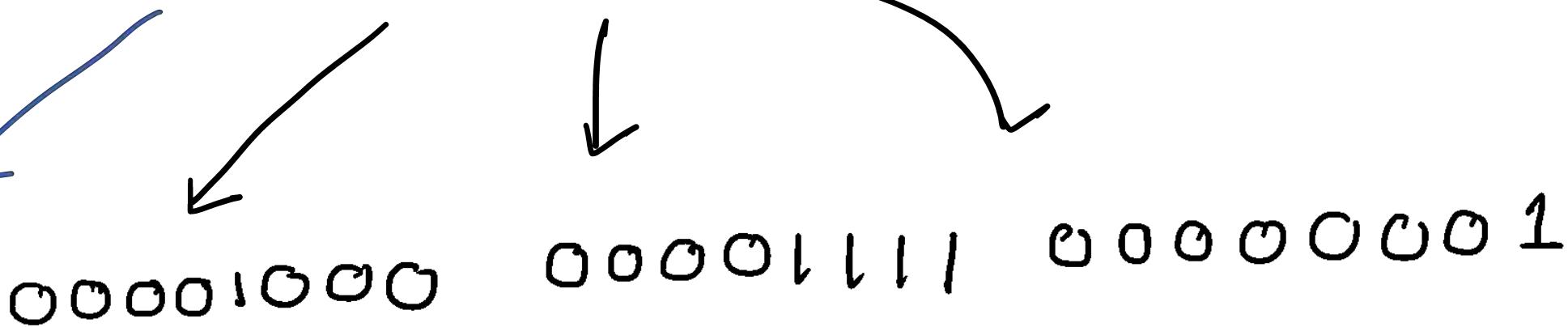
$$128 \cdot 8 \cdot 15 \cdot 1$$



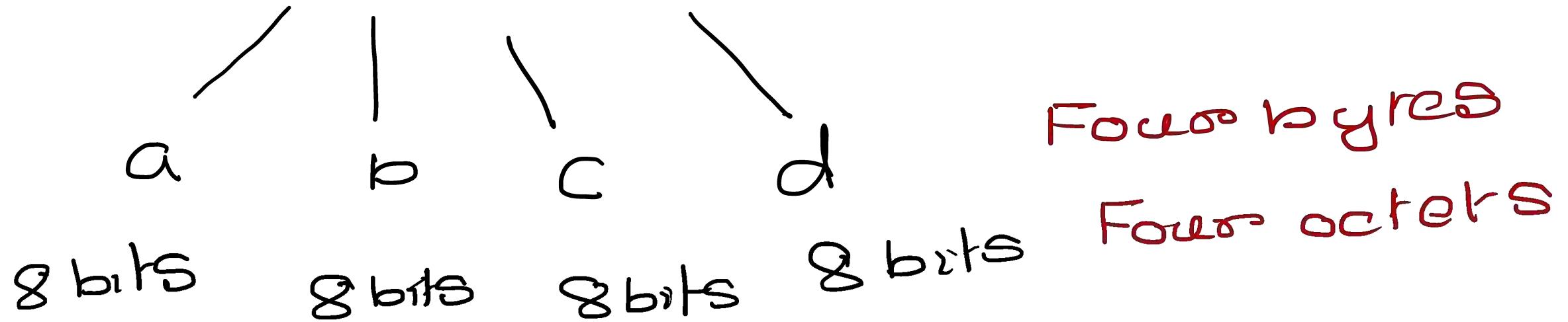
$$128 \cdot 8 \cdot 15 \cdot 1$$

00001000 00001111 00000001

$$128 \cdot 8 \cdot 15 \cdot 1$$



IPV4 \Rightarrow 32 bits long



Class C → 110 000000 → 192

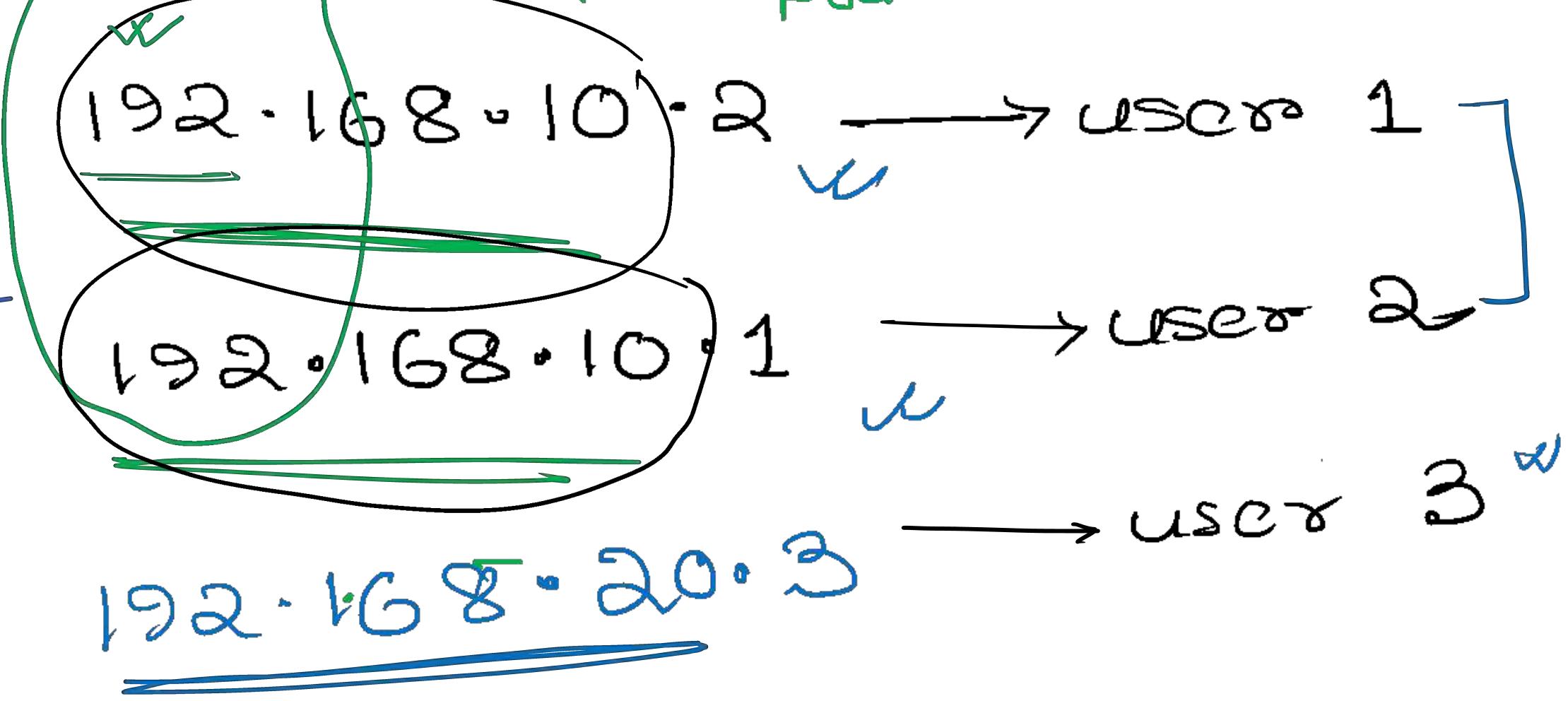
110 11111 → 223

Network portion Host portion
of IP address

192.168.10.2 ← user 1

255.255.255.0

N N N H



User 1 & user 2 belongs to
same network

Class A \Rightarrow 0 to 127 \Rightarrow 255.0.0.0

Class B \Rightarrow 128 to 191 \Rightarrow 255.255.0.0

Class C \Rightarrow 192 to 223 \Rightarrow 255.255.255.0

First byte/octet

0 00000000

First octet remaining bits are 3 octets

0 11111111

2⁷ \Rightarrow combinations each

128 network
16 hosts

network

8 bits \times 3 =

24 bits \Rightarrow host ad

2²⁴ - 2 hosts

Class C \Rightarrow 192 to 223 \Rightarrow $255 \cdot 255 \cdot 255 \cdot 0$

First octet

11000000
11011111

First 3 bits vs reserved
to define the class

remaining 5 bits here

$$5 + 8 + 8 = 21$$

$$2^{21} \Rightarrow \text{networks}$$

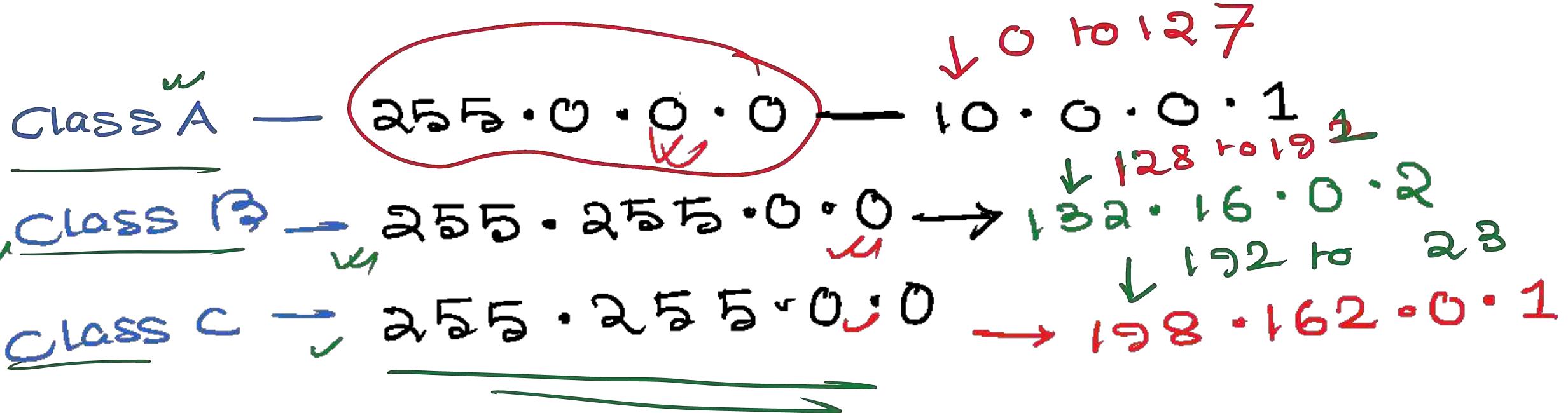
$$2^8 - 2 \Rightarrow$$

====

hosts

==== gateway

==== broadcast



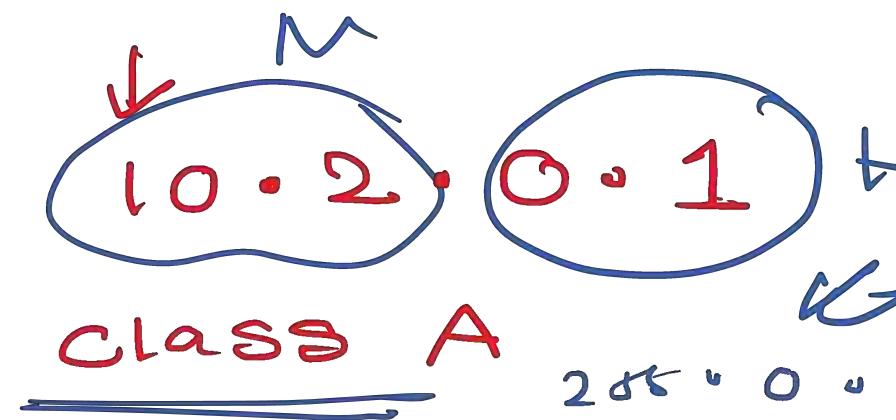
Class A \Rightarrow subnet mask of class B & C

Class B \Rightarrow subnet mask C

Class C \Rightarrow subnet mask G

A red oval encloses the first three octets of the subnet mask 255.255.0.0. An arrow points from this oval to the label "class C". Below it, the subnet mask is shown as 255.255.0.0 - 255.255.255. This indicates that the first three octets remain unchanged (255.255.0), while the fourth octet ranges from 0 to 255.

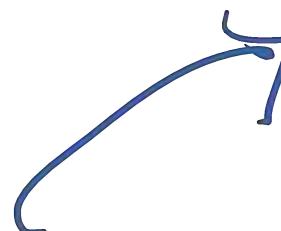
IP \Rightarrow addresses For user 1



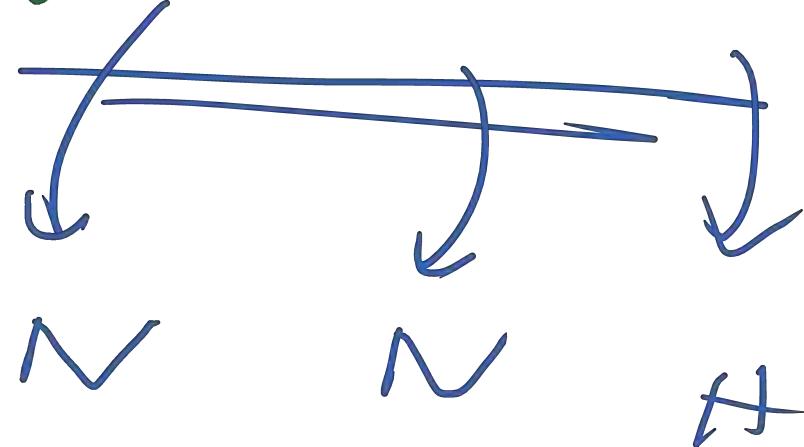
Given subnet mask

255.255.0.0

class B



255.255.0.



Q. user 1 have an IP address

172.16.200.1

user 2 " "

172.16.165.2

Subnet mask used is

255.255.255.1
N N N

Can we connect user 1 & user 2 with a swi



So to belong to same network user 1 &

~~users~~ the first 3 byte/octet should be same

Now belongs to same network we
cannot connected 1 & 2 user

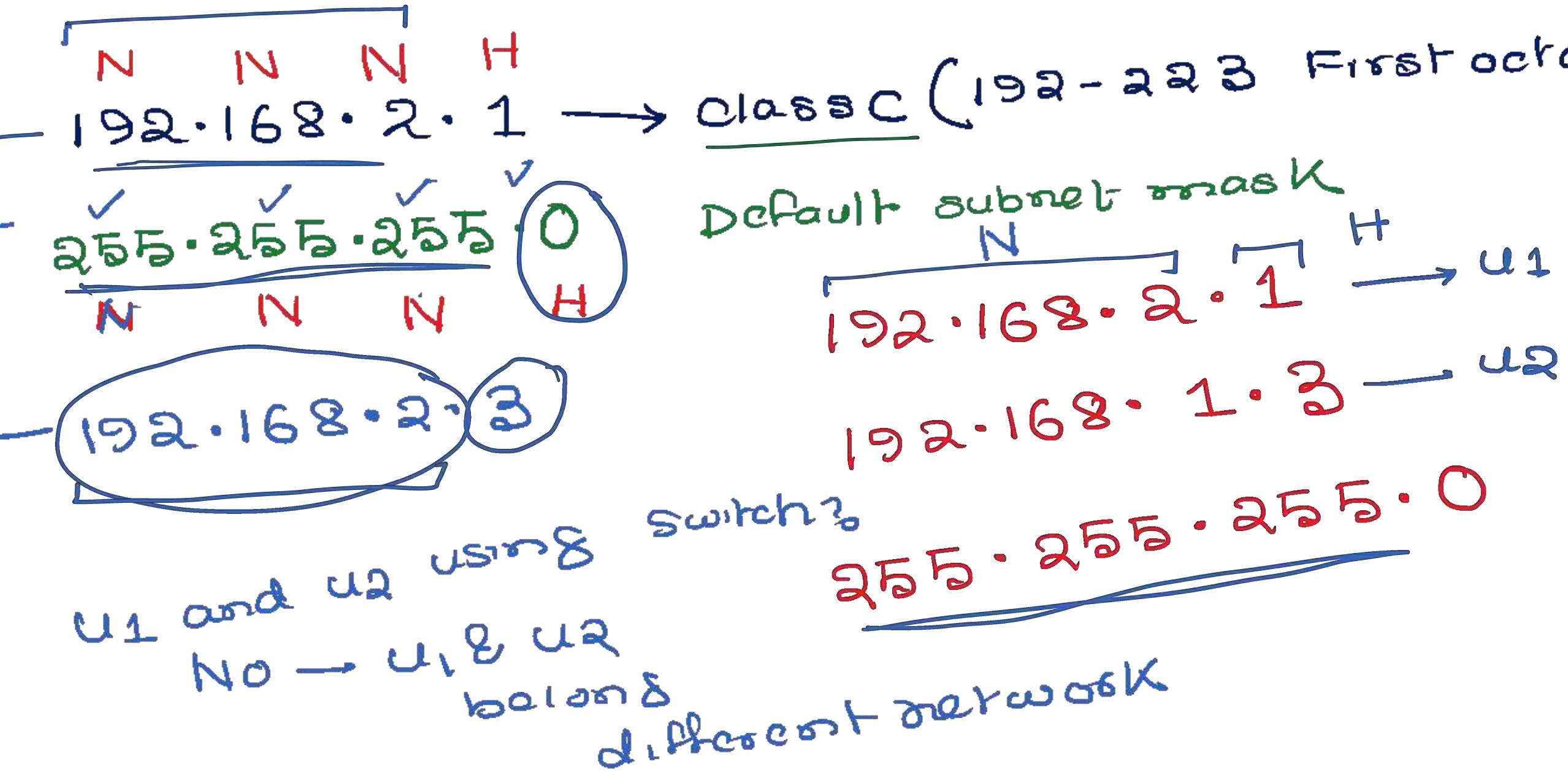
User 1 → 172 · 16 · 200 · 1] same network
User 2 → 172 · 16 · 165 · 2]
User 1 & User 2

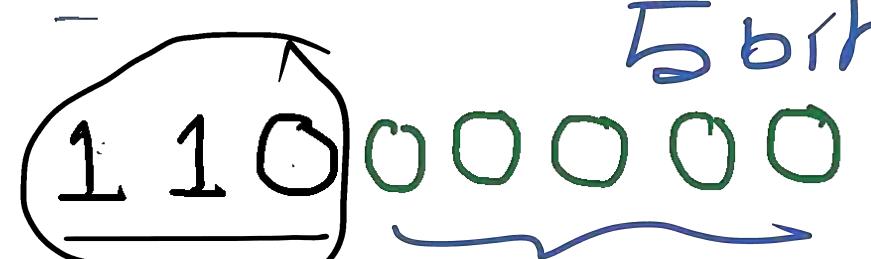
subnetmask_ 255 · 255 · 0 · 0
used vs N N H H

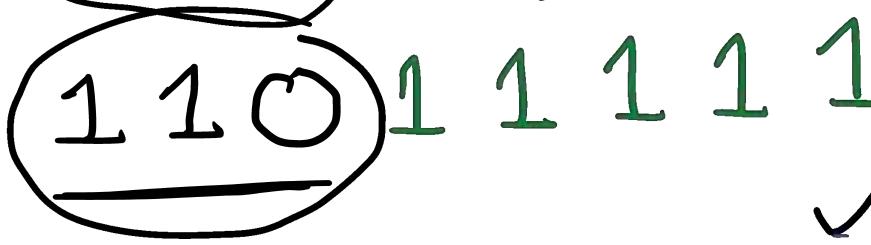
can be connected through switch
do not ->



Net. (Subnet) Host Port
 0 → 8 bits 8 bits 8 bits
 ✓
Class A → 0 0000000 → 0 ^w
 ✓
255.255.255.0 Broadcast → 1 1111111 → 127 ^w
 ✓
128 bloc
 Network = $2^7 = \cancel{128}$ ^{one}
 In each network
 Host = $(2^{24} - 2)$ ^{≈ 16 cores}
 Default subnet mask
 = 255.0.0.0 (class A)
 Service A = 10.2.1.0 (class A)
 IPV4 → 32 bits → 4 octets / 4 bytes



Class C :
 110  → 192

110  → 223

Default subnet mask = ~~255.255.255.255~~ = 0

Network address = $(5 + 8 + 8) = 21 = 2^{21}$

Host address = $2^8 - 2 = 254$

Class A → Default → class B &
Subnetmask class C

Class B → Default → class C
subnet mask

Higher class subnet mask
can be used

$\boxed{10 \cdot 1 \cdot 1 \cdot 2} \rightarrow$ class A

$\underline{\underline{255 \cdot 255 \cdot 255 \cdot 0}} \rightarrow$ subnet
mask for
class C.

Dotted Second

class A → 255 · 0 · 0 · 0

Бюдже^т

8

11111111.0000

A thick red line forms a wavy path. It starts at the far left with a small upward hook, then dips down to form a shallow V-shape. After the dip, it rises sharply to a higher level, which it maintains with minor fluctuations until it ends at the far right with a small downward hook.

|||||||. Good morning!

1 1 1 1) .) 1 1 1) . o o o o .

$$N \quad N \quad N \quad H$$

$$192 \cdot 168 \cdot 10 \cdot 1$$

mask

~~26~~

$$\begin{array}{r}
 128 \\
 + 6 \\
 \hline
 19
 \end{array}$$

subnet mask

$$192 \cdot 168 \cdot 10 \cdot 1$$

$$11111111 \cdot 11111111 \cdot 11111111 \cdot 110000$$

• 255 • 255 • 192 ←

255

$$130 \cdot 34 \cdot 12 \cdot 64 / 28$$

8 8

8 8 8 4

- 1 - - . 1 1 \cdot 1 1 - - 1 1 \cdot 1 1 1 1 0 0 0 0

255 \cdot 255 \cdot 255 \cdot 240

class C

\downarrow K

$$128 \\ 64 \\ 32 \\ 16$$

28 - 2

5 + 8 + 8

$$\rightarrow 100 \cdot 10 \cdot 5 \cdot 2 \rightarrow \text{U1}^w$$

$$- 100 \cdot 10 \cdot 5 \cdot 5 \rightarrow \text{U2}^w$$

$$100 \cdot 10 \cdot 5 \cdot 6 \rightarrow \text{U3}^w$$

$$255 \cdot 255 \cdot 255 \cdot 252 \rightarrow$$

$\underbrace{\quad\quad\quad}_{2}$ $\overbrace{\quad\quad\quad}^{+1}$

subnet
maske

$u_1 \rightarrow 100 \cdot 10 \cdot 5 \cdot 2 \rightarrow 01100100$ $00001010 \cdot 000000$
 $255 \cdot 255 \cdot 255 \cdot 252$

$\rightarrow 11111111 \cdot 11111111 \cdot 11111111 \cdot 11111111$

AND operation =

$01100100 \cdot 00001010 \cdot 00000101 \cdot 000000$

$= 100 \cdot 10 \cdot 5 \cdot 0 \rightarrow u_1 \rightarrow \underline{\text{dilfere}}$
 $100 \cdot 10 \cdot 5 \cdot 4 \rightarrow u_2$ same
 $100 \cdot 10 \cdot 5 \cdot 4 \rightarrow u_3$

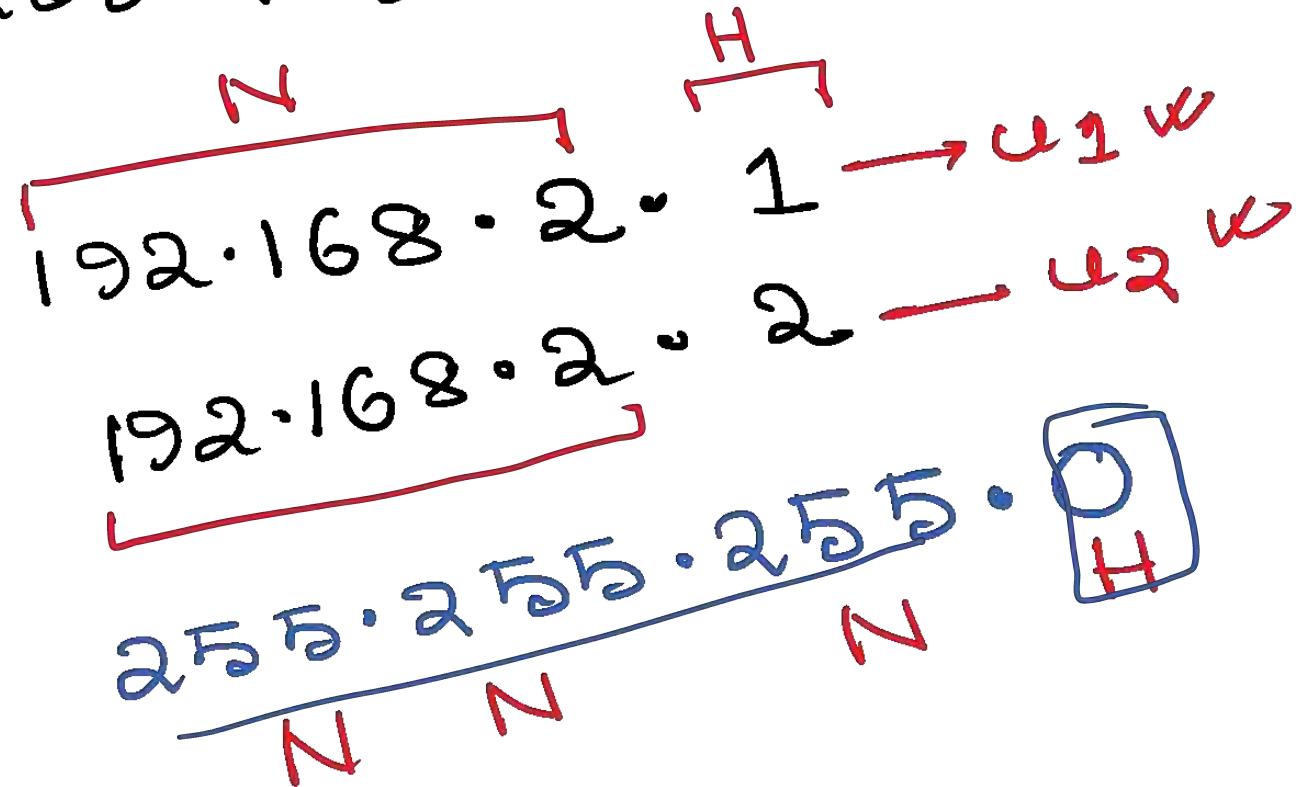
O ← Network (Gateway)

Q. 255 → Subnet mask of class B & C
- broadcast

Class B → Subnet mask of class C
Fist byte/ Octet class C

The diagram illustrates the structure of a Class C IP address and its subnetting. At the top left, a red oval labeled "Class C" has an arrow pointing to a binary number $110\ 000000$. This is converted to the decimal value 192. To the right, a formula $(5+8+8) = 2^2 + 2^1 \rightarrow 7$ is shown, indicating the number of possible subnets. Below this, a red box highlights the first three bits of the original binary number as 110, which is converted to the decimal value 223. A green bracket labeled "8 bits" indicates the range of values for each network. The bottom part shows the standard octet representation of an IP address: $255 \cdot 255 \cdot 255 \cdot 0$. The last octet is circled in green and has an arrow pointing to it from the "8 bits" label.

$255 \cdot 255 \cdot 255 \cdot 255$



uv & ua with
switch Host w/
Host w/
~~192.168.2.0~~
~~192.168.2.255~~

~~3~~

$$U_1 \rightarrow 100 \cdot 10 \cdot 5 \cdot 2^w \cdot 3^w$$

$$U_2 \rightarrow 100 \cdot 10 \cdot 5 \cdot 5^w$$

$$U_3 \rightarrow 100 \cdot 10 \cdot 5 \cdot 6^w$$

Subtotal: ~~100~~

$$255 \cdot 255 \cdot 255 \cdot 255 \cdot 252$$

N_1	2^6	N_2	2^{25}	N_3	2^{4N}	2^3	2^2	2^1	2^0
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^0	2^0
128	64	32	16	8	4	2	1	x	x

$10 \cdot 5 \cdot 2 \rightarrow 011001000000101000000101000000$

mask $\rightarrow 111111111111111111111111111111111111111$

answer $\rightarrow 011001000000101000000101000000$

$10 \cdot 5 \cdot 0$

$U_1 \rightarrow 100 \cdot \dots$

$$\overbrace{130 \cdot 34 \cdot 12 \cdot 64}^{\text{Host}} / 28 \leftarrow \begin{array}{l} \text{subnet mask} \\ \text{128} \end{array}$$

IP V4

addresses
accompanied addresses
net mask

2 acc
 only mask
 $11111111 \cdot 11111111 \cdot 11111111 \cdot 1111100000$
 $\rightarrow 255 \quad c \quad 255 \quad \cdot \quad 255 \quad \cdot \quad 240$
 $\underline{N} \quad \underline{N} \quad \underline{N} \quad \underline{H}$

$2^8 - 2 = 256 - 2 = 254$ no. hosts can be possible

130.34.12.0 ← network address (gateway)

- 130.34.12.255 ← Broadcast address

6 .
N N H H

192.168.20.1 → class B
default subnet

255.255.0.0

mask

network = 2^{14} ✓

10 0000000

Module 3

Network Layer ➤ Subnetting



Dr. Sunandita Debnath, IIIT Vadodara

Different ways of Transmission in IPV4

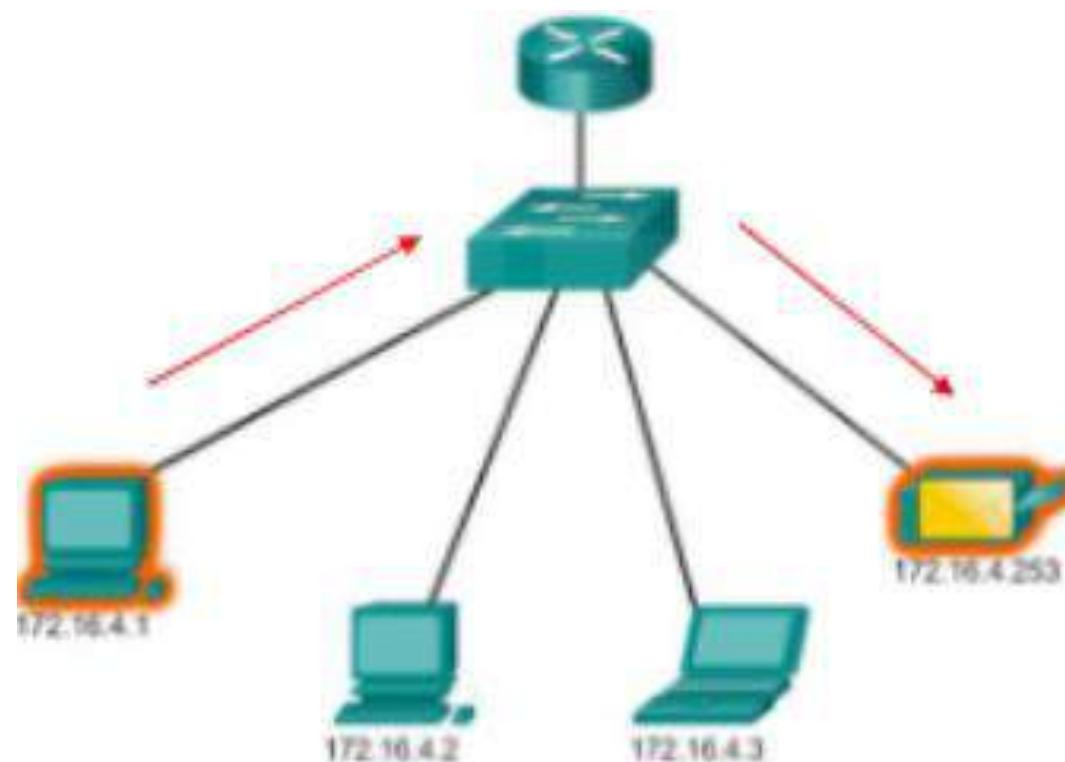
➤ In a IPV4 network, the hosts communicate one of three different ways

- Unicast*
- Broadcast*
- Multicast*

Unicast Transmission: *The process of sending a packet from one individual host to another host.*

Source: 172.16.4.1

Destination: 172.16.4.253



Different ways of Transmission in IPV4

Broadcast Transmission: *The process of sending a packet from one host to all hosts in the network.*

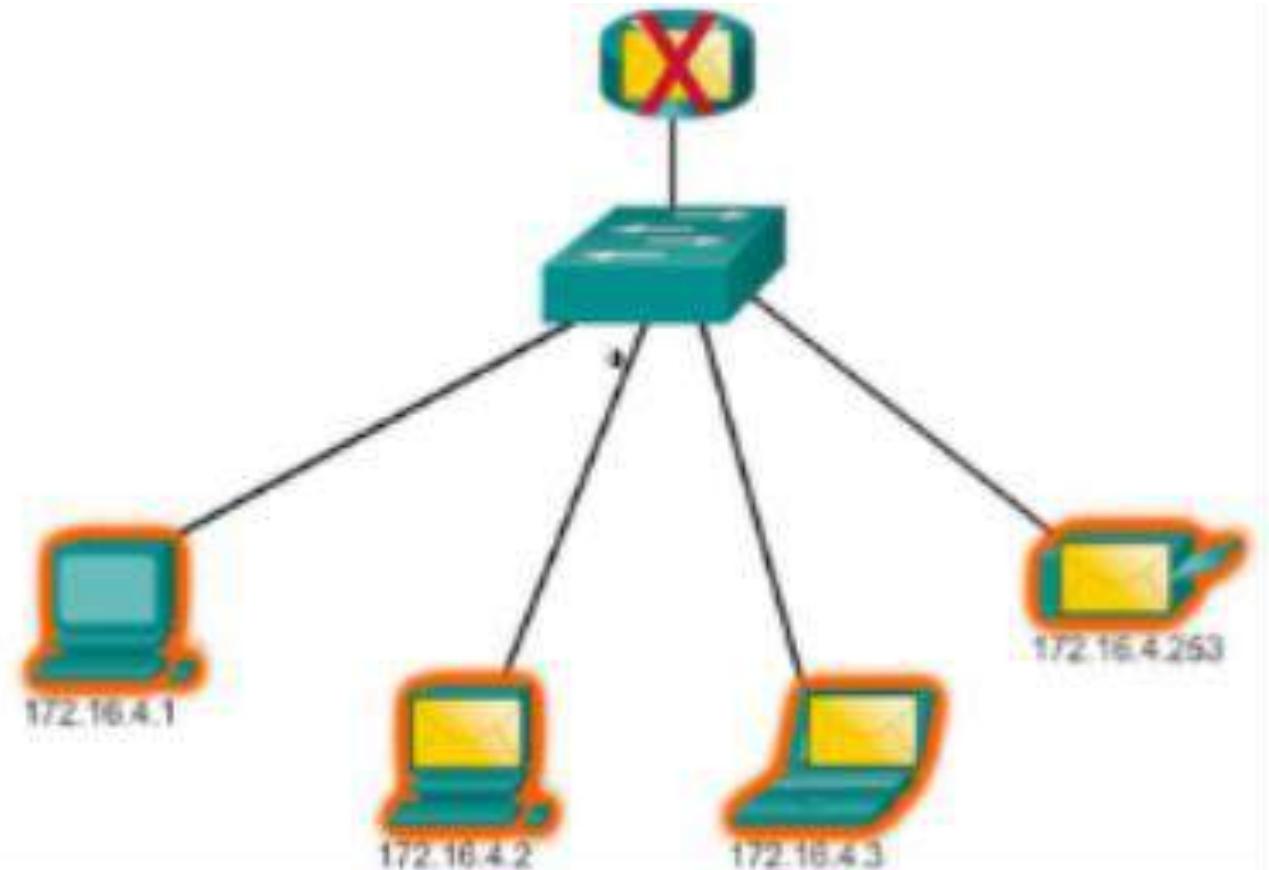
- Limited Broadcast*
- Directed Broadcast*

Limited Broadcast

Source: 172.16.4.1

Destination: 255.255.255.255

Router will not forward a limited broadcast.



Directed Broadcast

Destination: 172.16.4.255

Host within the 172.16.4/24 network

Different ways of Transmission in IPV4

Multicast Transmission: *The process of sending a packet from one host to a selected group of hosts, possibly in different networks.*

- *Multicast transmission reduces traffic*
- *The multicast address range 224.0.0.0 to 239.255.255.255.*
- *Link Local-224.0.0.0 to 224.0.0.255 (E.g. routing information exchanged by routing protocols)*
- *Globally scoped address-224.0.1.0 to 238.255.255.255 (E.g. 224.0.1.1 has been reserved for Network Time Protocol)*

Public and Private IPV4 Addresses

Private IP addresses:

- *IPV4 address ranges from 0.0.0.0 to 255.255.255.255, where 0.0.0.0 is the network address and 255.255.255.255 is the broadcast address.*
- *According to early network design, IP addresses should be unique, but this is not true with the introduction of private and public IP addresses.*
- *Two computers can use the same private address using NAT (Network Address Translation).*
- *Hosts that do not require access to the internet can also use private addresses. E.g. many computers in a company do not need internet connectivity but can communicate internally among each other using private IP addresses.*

Private IPV4 Addresses

- *Ranges of Private IP address*
 - 10.0.0.0 to 10.255.255.255 (10/8) Class A
 - 172.16.0.0. to 172.31.255.255 (172.16.0.0/12) Class B
 - 192.168.0.0 to 192.168.255.255 (192.168.0.0/16) Class C
- *The aforementioned are the three non overlapping ranges of IPV4 addresses for private networks are reserved.*
- *Public IP address is used to communicate outside the network. Public IP addresses are basically assigned by the Internet Service Provider (ISP)*

Special use IPV4 Addresses

❑ Network and Broadcast addresses

Within each network the last and first address can not be assigned to hosts.

❑ Loopback addresses **127.0.0.1 (127.0.0.0 to 127.255.255.255 are reserved)**

127.0.0.1 is a special address which hosts use to direct traffic to themselves

Link-Local addresses 169.254.0.0 to 169.254.255.255 (169.254.0.0/16)

Can automatically assigned to the local hosts.

Test-Net addresses 192.0.2.0 to 192.0.255.255 (192.0.2.0/24)

Set aside for teaching and learning purposes, used in documentation and network example.

❑ Experimental addresses **240.0.0.0 to 255.255.255.254**

Are listed as reserved for experimental purpose.

Drawbacks of Classful Addressing

Address Class	1st Octet range in decimal	1st Octet bits (Blue Dots do not change)	Network (N) and Host (H) Portion	Default mask (Decimal)	Number of possible networks and hosts per network
A	0-127	00000000 01111111	N.H.H.H	255.0.0.0	128 Nets (2^7) 16,777,214 hosts ($2^{24}-2$)
B	128-191	10000000 - 10111111	N.N.H.H	255.255.0.0	16,384 Nets (2^{14}) 65,534 hosts ($2^{16}-2$)
C	192-223	11000000 - 11011111	N.N.N.H	255.255.255.0	2,09,150 Nets (2^{21}) 254 hosts (2^8-2)
D	224-239	11100000 - 11101111	NA (Multicast)	-	-
E	240-255	11110000 - 11111111	NA (Experimental)	-	-

Drawbacks of Classful Addressing

- *Lack of Internal Address Flexibility*
- *Inefficient use of address space*
- *Proliferation of Router Table entries*

Classless Addressing

- *Formal name is Classless Inter-Domain Routing (CIDR).*
- *Created a new set of standards that allowed service providers to allocate IPV4 addresses on any address bit boundary (prefix length) instead of only Class A, B, and C addresses.*
- *Classless addressing is possible with the help of subnetting.*

Valid Subnet Masks

Valid Subnet Masks

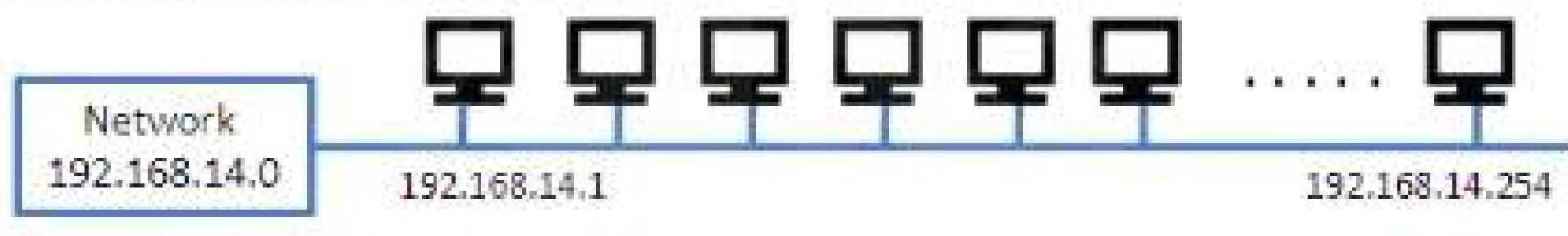
<i>/n</i>	<i>Mask</i>	<i>/n</i>	<i>Mask</i>	<i>/n</i>	<i>Mask</i>	<i>/n</i>	<i>Mask</i>
/1	128.0.0.0	/9	255.128.0.0	/17	255.255.128.0	/25	255.255.255.128
/2	192.0.0.0	/10	255.192.0.0	/18	255.255.192.0	/26	255.255.255.192
/3	224.0.0.0	/11	255.224.0.0	/19	255.255.224.0	/27	255.255.255.224
/4	240.0.0.0	/12	255.240.0.0	/20	255.255.240.0	/28	255.255.255.240
/5	248.0.0.0	/13	255.248.0.0	/21	255.255.248.0	/29	255.255.255.248
/6	252.0.0.0	/14	255.252.0.0	/22	255.255.252.0	/30	255.255.255.252
/7	254.0.0.0	/15	255.254.0.0	/23	255.255.254.0	/31	255.255.255.254
/8	255.0.0.0	/16	255.255.0.0	/24	255.255.255.0	/32	255.255.255.255

Subnetting

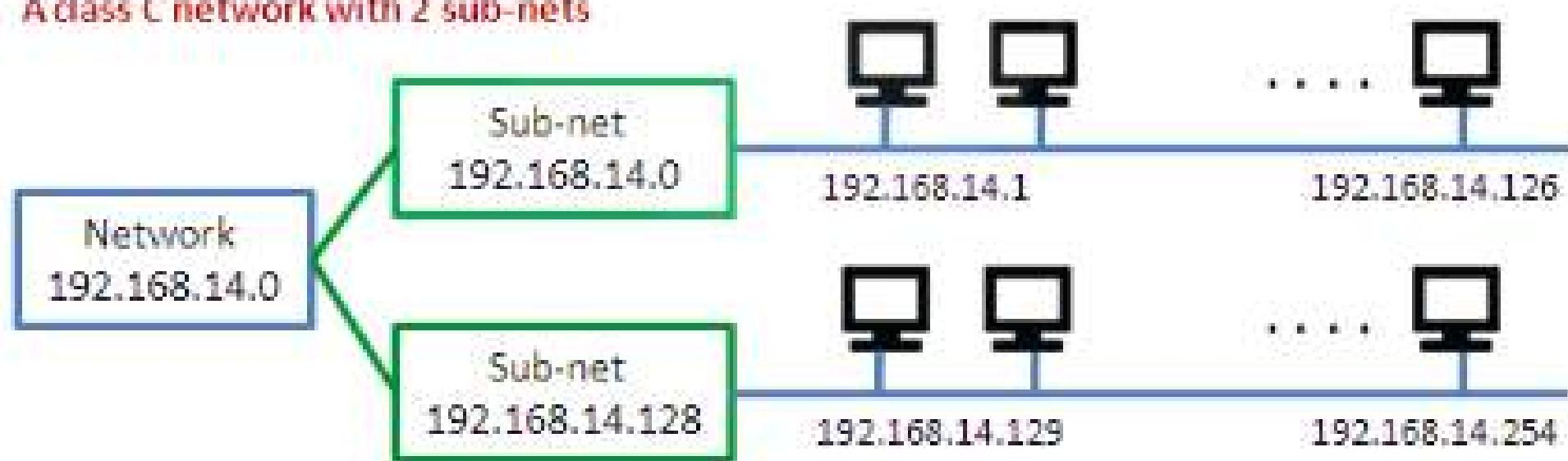
- A *subnetwork or subnet is a logical subdivision of an IP addresses.*
- *The practice of dividing a network into two or more networks is called subnetting.*
- *Computers that belongs to a subnet are addressed with an identical most significant bit-group in their IP addresses.*

IP Subnetting Example

A class C network without sub-netting



A class C network with 2 sub-nets



- The first address and the last address is reserved for network and broadcast respectively. The default subnet mask for Class C which is 255.255.255.0 cannot be used for subnetworks. But the total number of host supported by Class C ie.e $2^8 - 2 = 254$ should be maintained.

Subnetting

Subnetting can be done both according to Host requirement and network requirement.

The steps for subnet the given network according to host requirements:

- Identify the Class of the IP address and note the default subnet mask.*
- Convert the default subnet mask into binary format.*
- Note the number of hosts required per subnet and find the binary equivalent of it.*
- Find the subnet generator (SG) and octet position.*
- Generate the new subnet mask.*
- Use the SG and generate the network ranges in the appropriate Octet positions.*

Q. Subnet the IP address 216.21.5.0 into 30 hosts in each subnet.

Q. Subnet the IP address 196.10.20.0 into 52 hosts in each subnet.

Q. Subnet the IP address 150.15.0.0 into 500 hosts in each subnet.

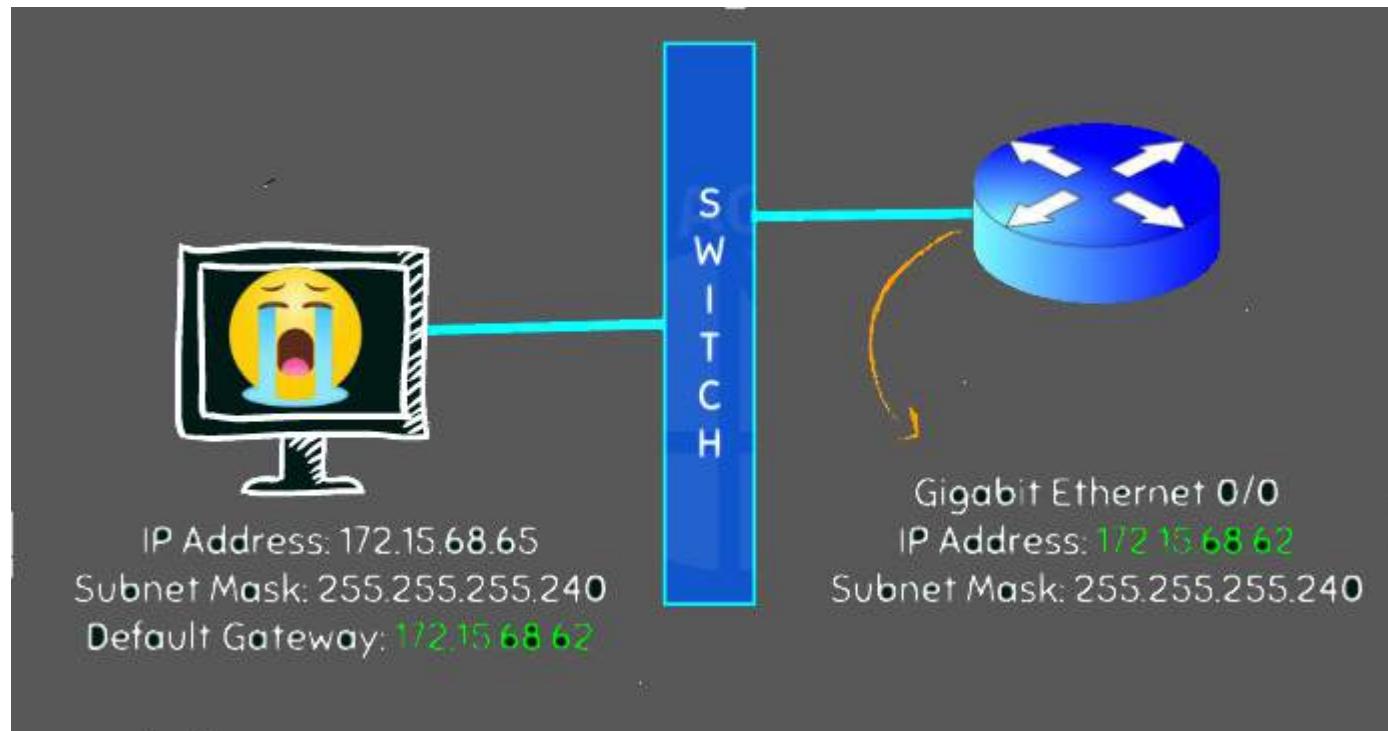
Q. Subnet the IP address 10.0.0.0 into 100 hosts in each subnet.

Trouble shooting in Subnetting

A computer is assigned with an IP address 192.168.1.127 and subnet mask 255.255.255.224. But the computer is not able to communicate with the PCs in the network, why?

Trouble shooting in Subnetting

A computer is assigned with an IP address 172.15.68.65 and subnet mask 255.255.255.240 and the default gateway for connecting to the internet or other computer in different is 172.15.68.62. But the computer is not able to communicate with the PCs in the other network, why?



Module 3

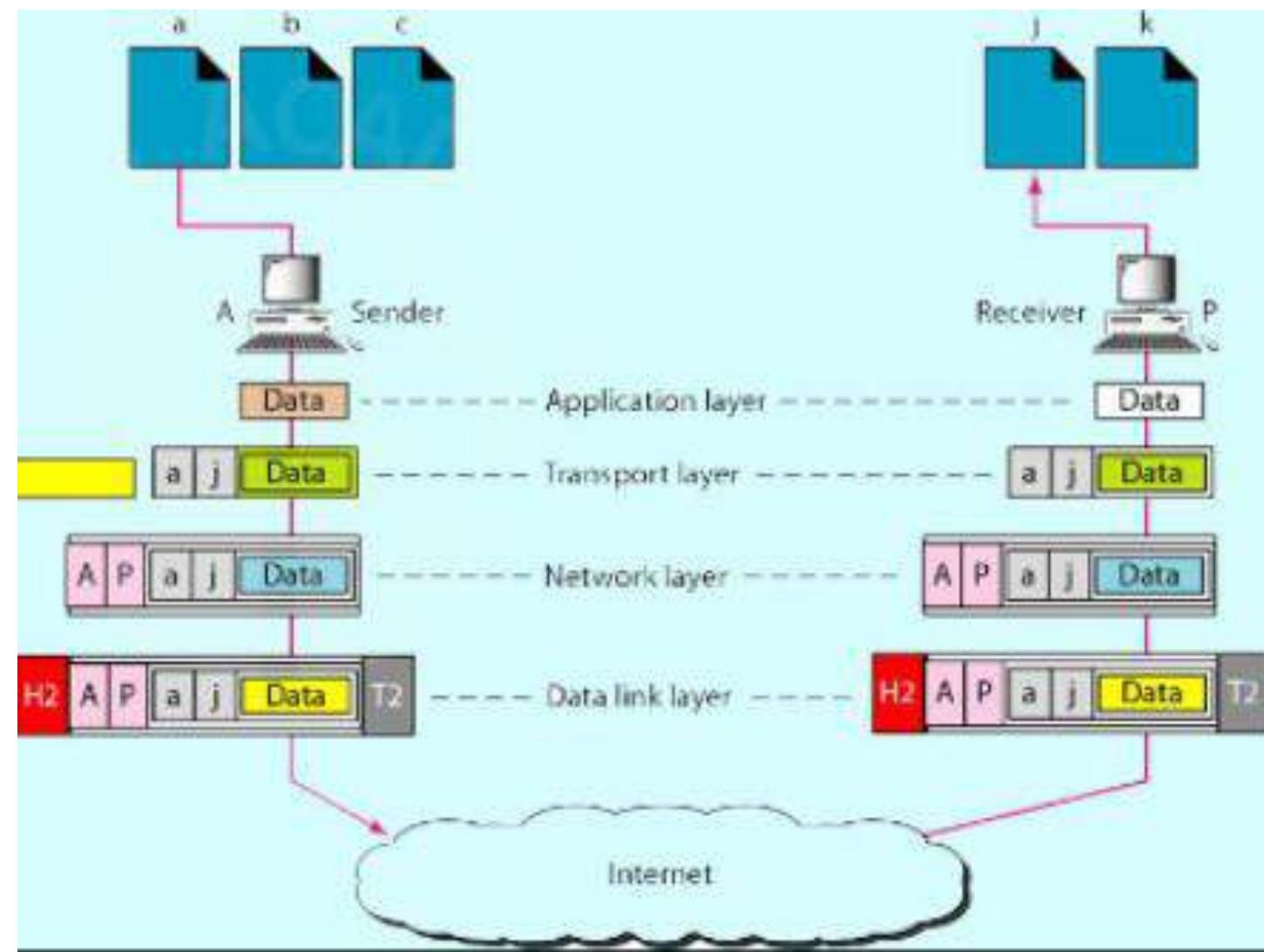
Network Layer protocols



Dr. Sunandita Debnath, IIIT Vadodara

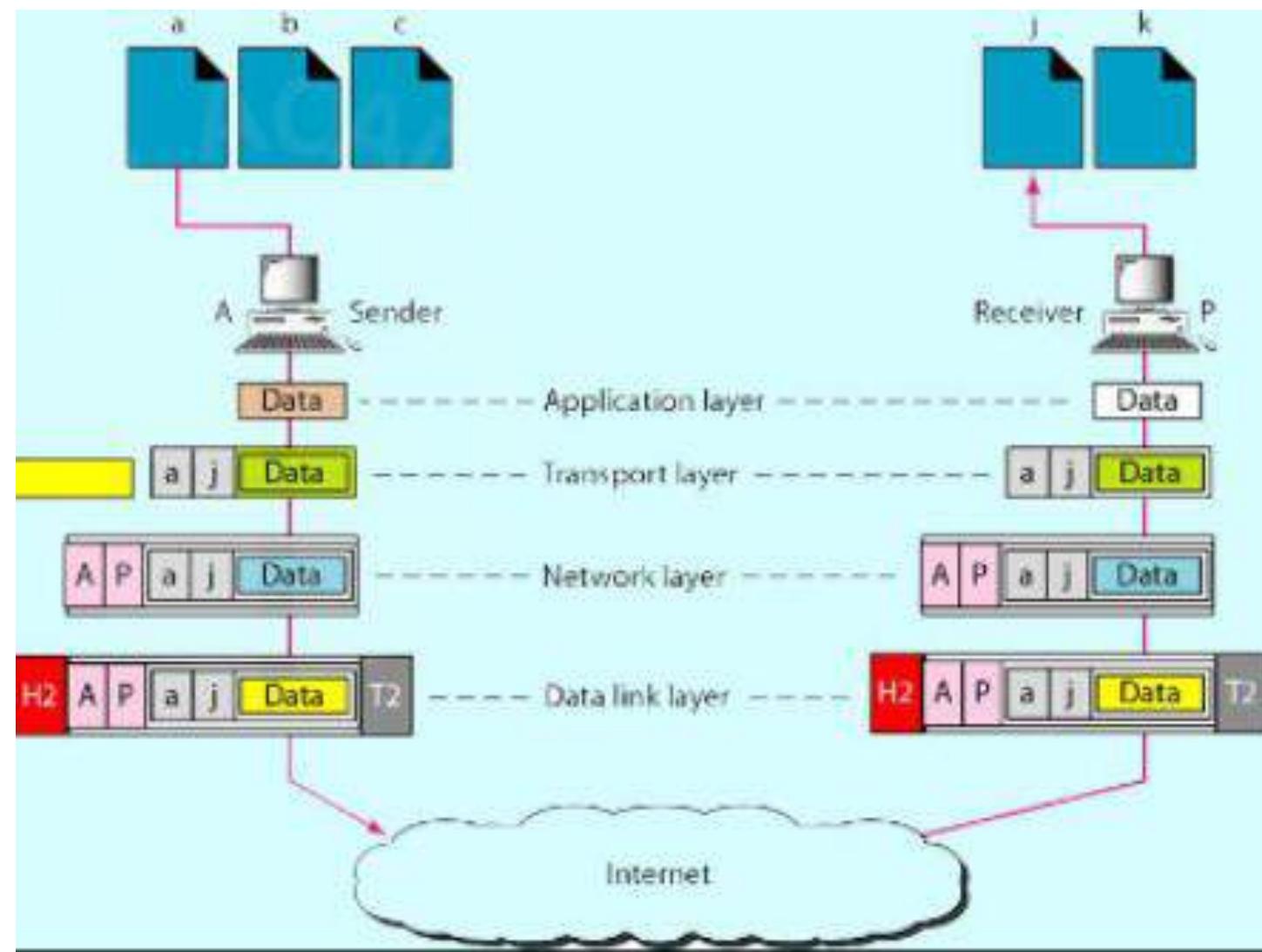
Different ways for Communication

- *Transport layer deals with port addressing, Port no is of 16 bits (0 to 65535)*
- Well known ports (0 to 1023)
- Registered ports (1024 to 49151)
- Dynamic or private ports (49152 to 65535)



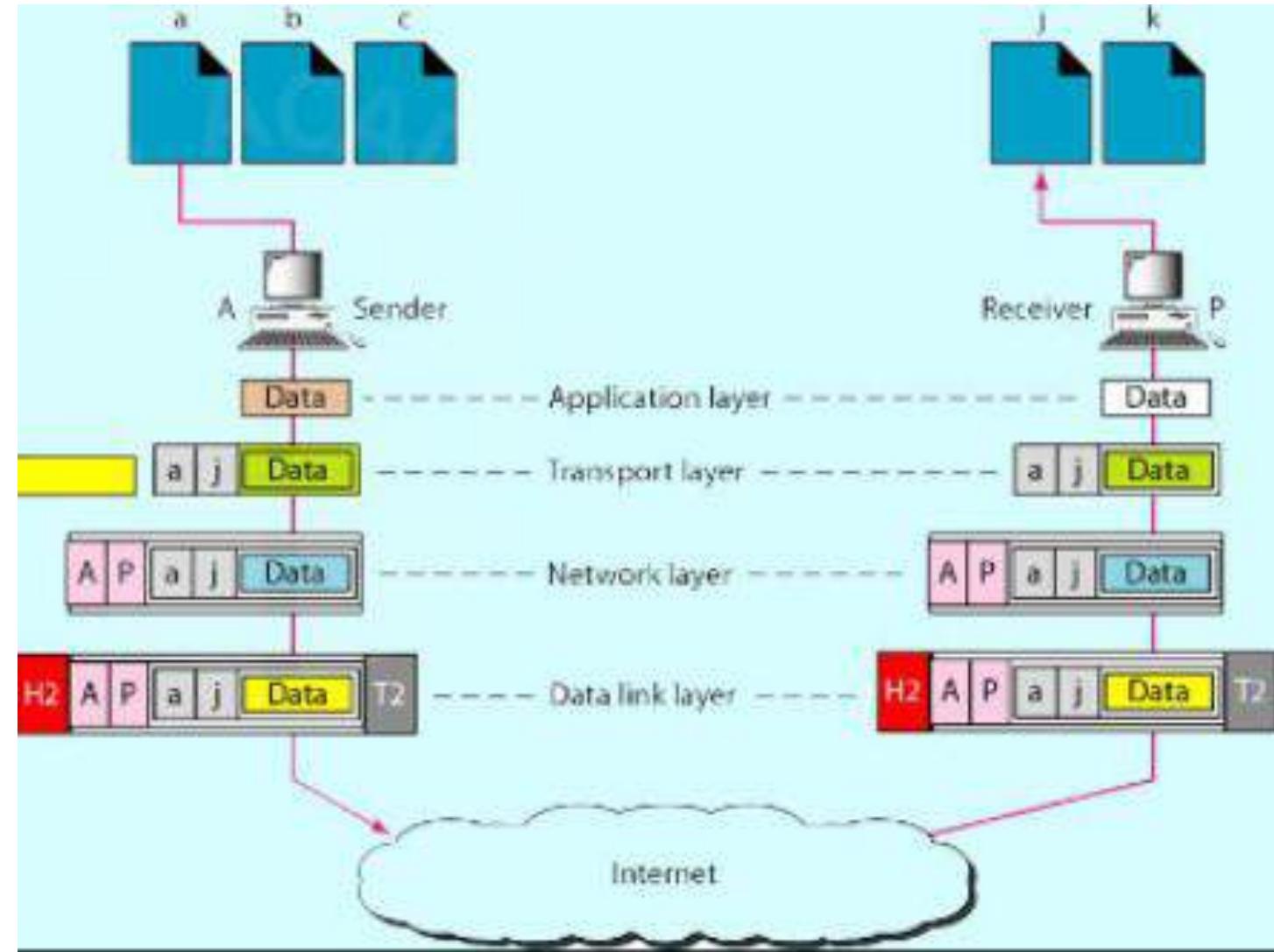
Different ways for Communication

- Network layer or Internet layer deals with IP addresses IPV4 addresses are 32 bits and IPV6 addresses are 128 bits long (Hexadecimal).
- Either user provides the IP addresses or DNS resolves the names into IP addresses.

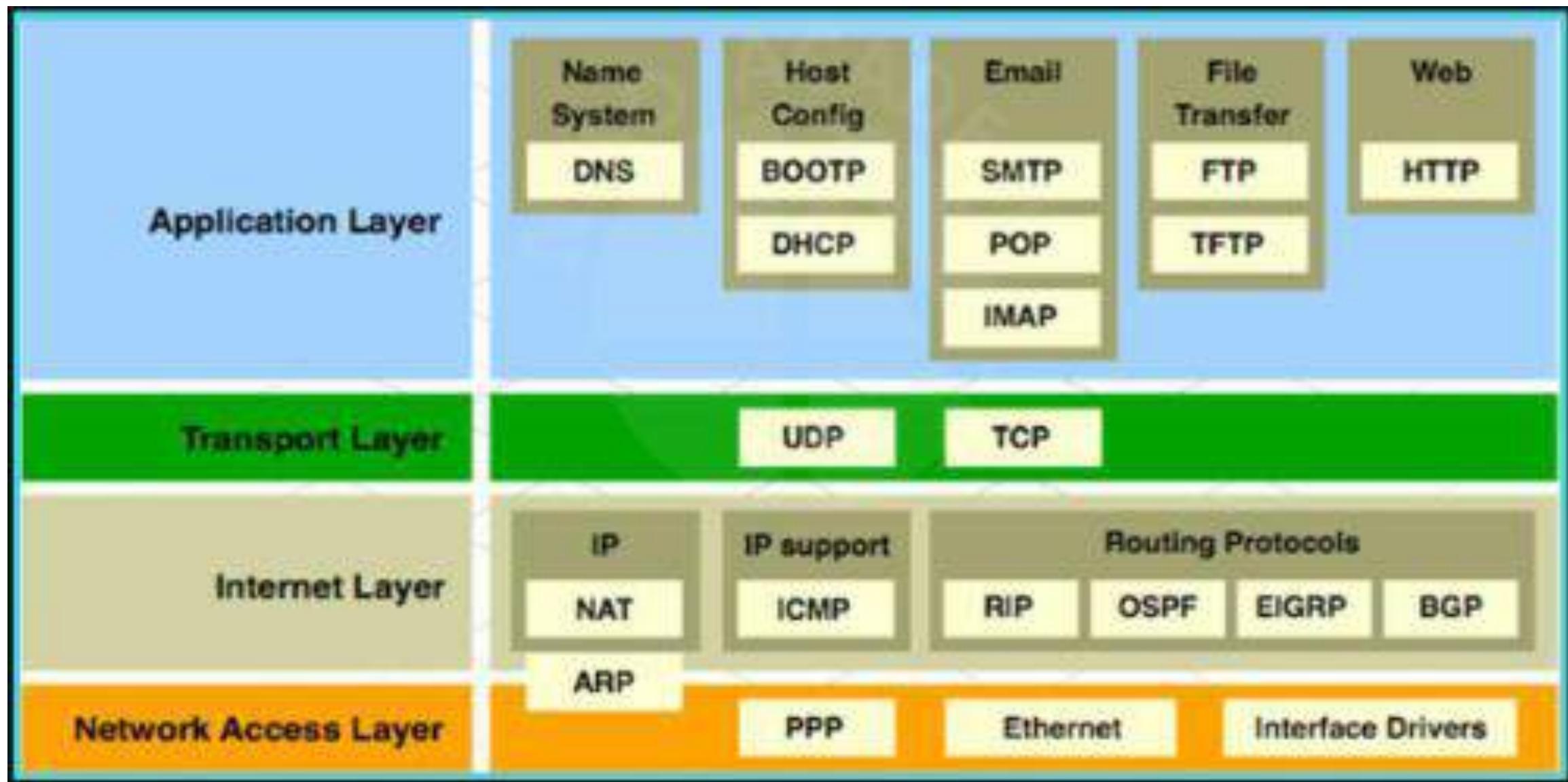


Different ways for Communication

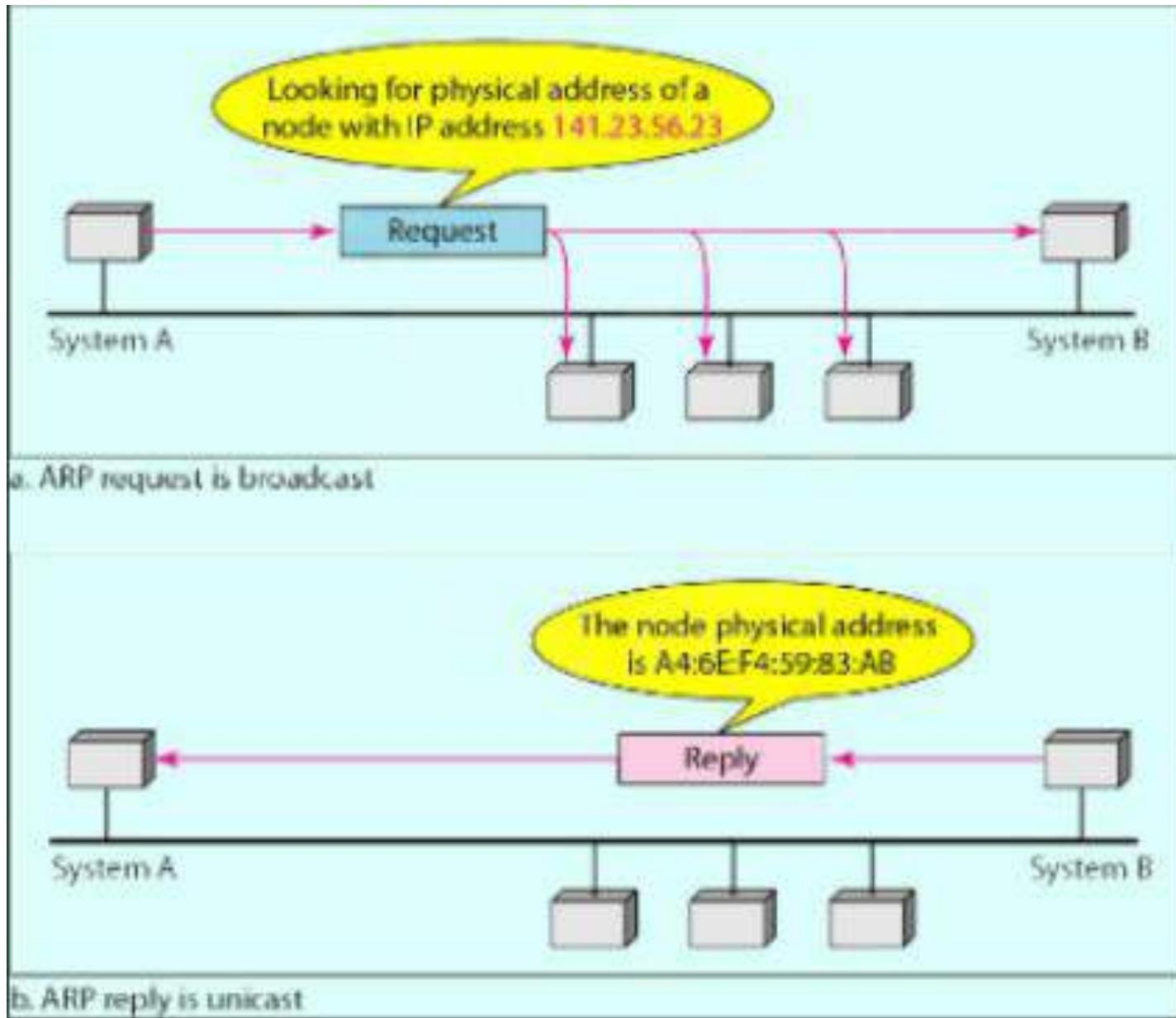
- Data link deals with MAC addresses or hardware addresses. *MAC addresses are 48 bits long (Hexadecimal).*
- Assigned by manufacturer and usually wont be changed.
- *The mapping between the IP address and the MAC address is done by the ARP (Address Resolution Protocol).*



TCP/IP suite



Address Resolution Protocol (ARP)



ARP Protocol

The ARP protocol provides two basic functions:

- *Resolving IPV4 address to MAC address.*
- *Maintaining a table of mapping.*

ARP Protocol

- *ARP maintains a cache of IP addresses and MAC addresses.*
- *ARP request is sent with an broadcast MAC address FFFF.FFFF.FFFF if the IP address is not in the table.*
- *Target machine responds (unicast) with its physical address.*
- *Table entries are discarded if not refreshed.*

Header of ARP Packet

0	8	16	31
Hardware type=1		ProtocolType=0x0800	
HLen=48	PLen=32	Operation	
SourceHardwareAddr (bytes 0–3)			
SourceHardwareAddr (bytes 4–5)		SourceProtocolAddr (bytes 0–1)	
SourceProtocolAddr (bytes 2–3)		TargetHardwareAddr (bytes 0–1)	
TargetHardwareAddr (bytes 2–5)			
TargetProtocolAddr (bytes 0–3)			

Header of ARP Packet

- ***Hardware Type:*** *Type of Physical network (i.e. Ethernet)*
- ***Protocol Type:*** *Type of upper layer protocol (e.g. IP)*
- ***HLEN and PLEN:*** *Length of physical address and Protocol address*
- ***Operation:*** *ARP Request or a ARP Reply*
- *Source Physical address /Protocol address & Target Physical address /Protocol addresses*

RARP Protocol

The ARP protocol provides two basic functions:

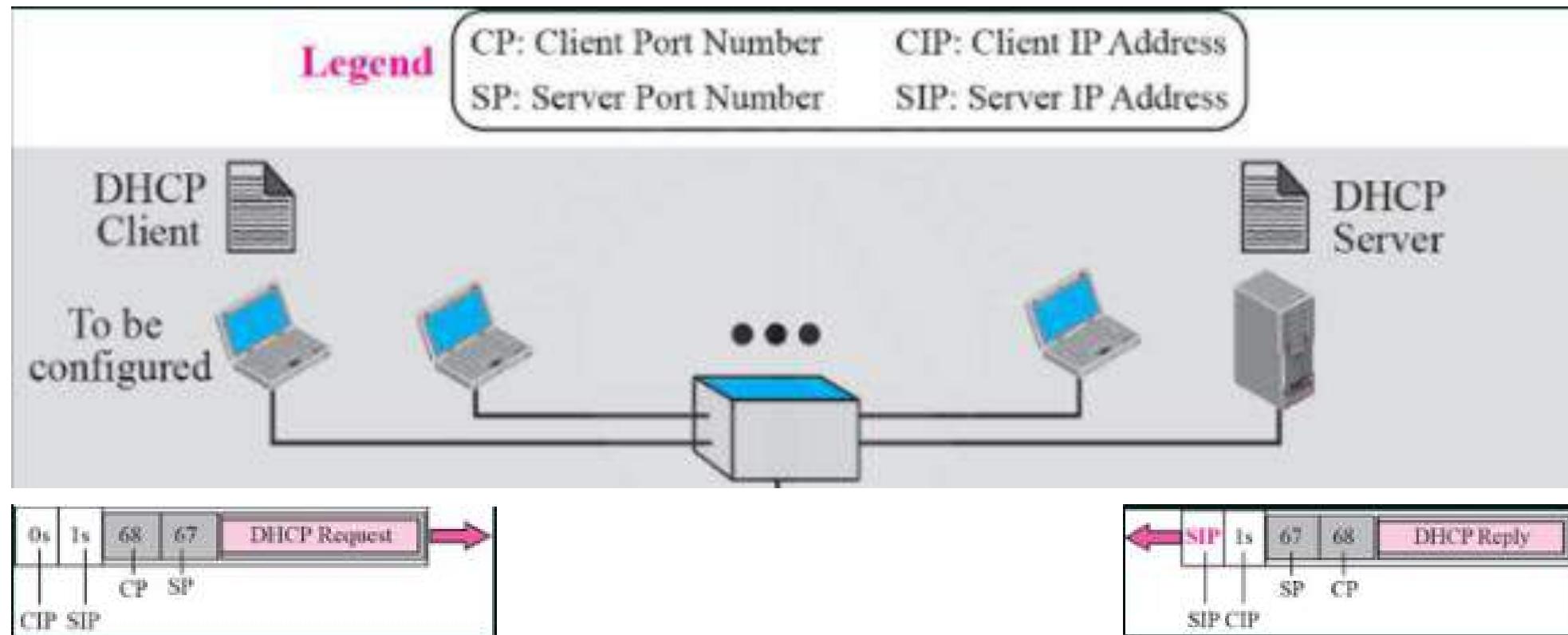
- *Reverse ARP (RARP) is an obsolete computer networking protocol used by a client computer to request its internet protocol address from a computer network, when all it has available is its link layer or hardware address, such as MAC address.*
- *The protocol can use the known MAC address to retrieve its IP address. Functionality wise, RARP is the complete opposite of ARP. The RAP uses the known IP address to determine the MAC address of the computer.*
- *It has been rendered obsolete by the Bootstrap protocol (BOOTP) and the modern dynamic host configuration protocol (DHCP), which both support a much greater feature set than ARP.*
- *The RARP cannot handle subnetting because no subnet masks are sent. If multiple subnets are deployed, an RARP server must be available in each subnet.*

DHCP

- ❑ *Dynamic Host Configuration Protocol .*
- ❑ *The MAC addresses are configured into network by manufacturer and they are expected to be unique.*
- ❑ *IP addresses must be unique in a inter-network. Most operating system provide away to manually configure the IP information for the host.*
- ❑ *Drawback of manual configuration:*
A lot of work to configure all the hosts in a large network.
Configuration process is error prone.
- ❑ *Hence automated IP configuration is required.*

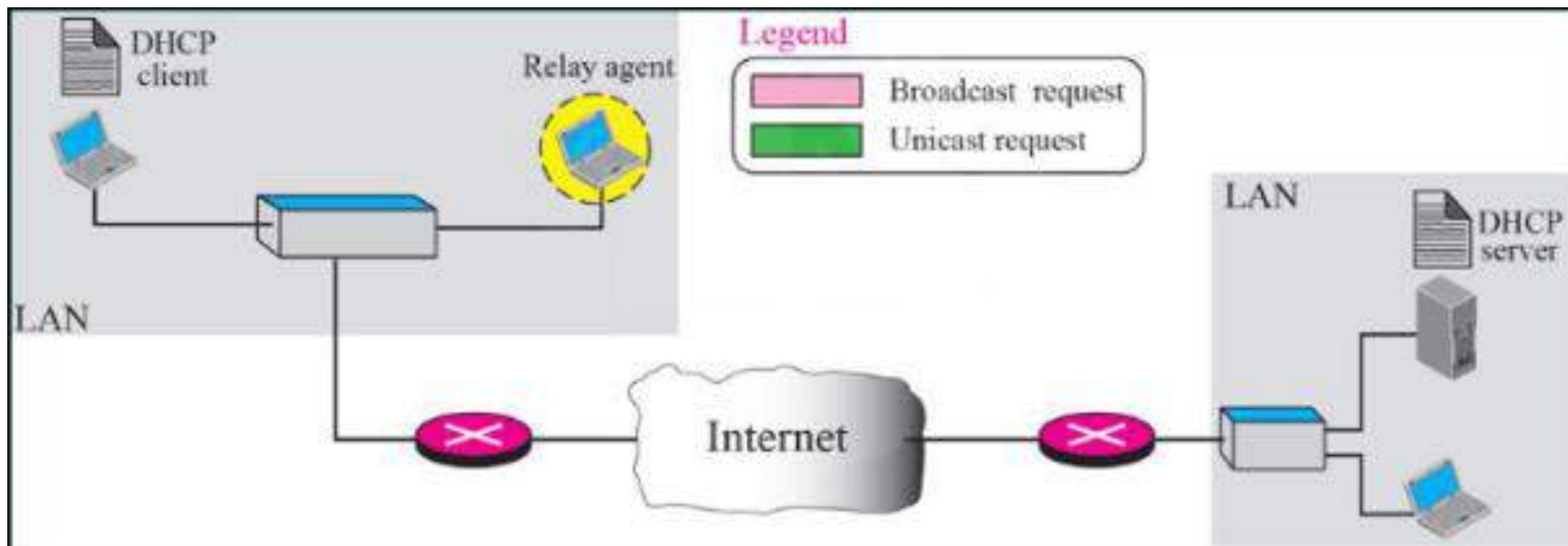
DHCP

DHCP server and Host in same network



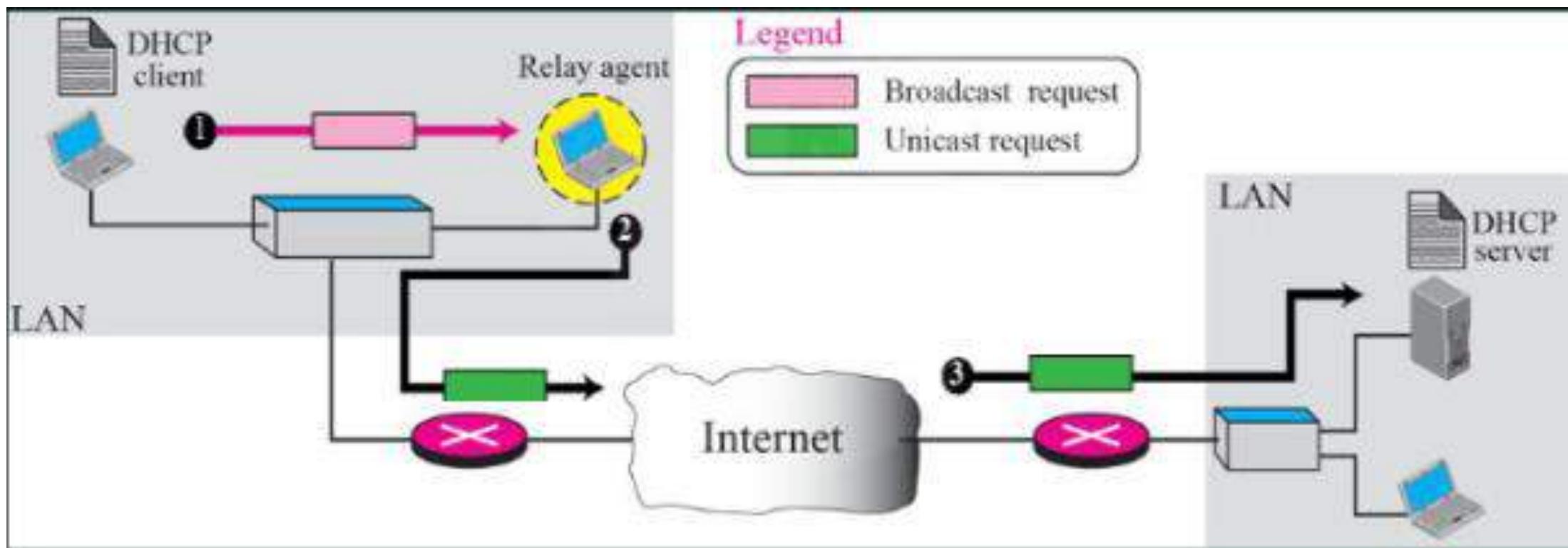
DHCP

DHCP server and Host in Different network



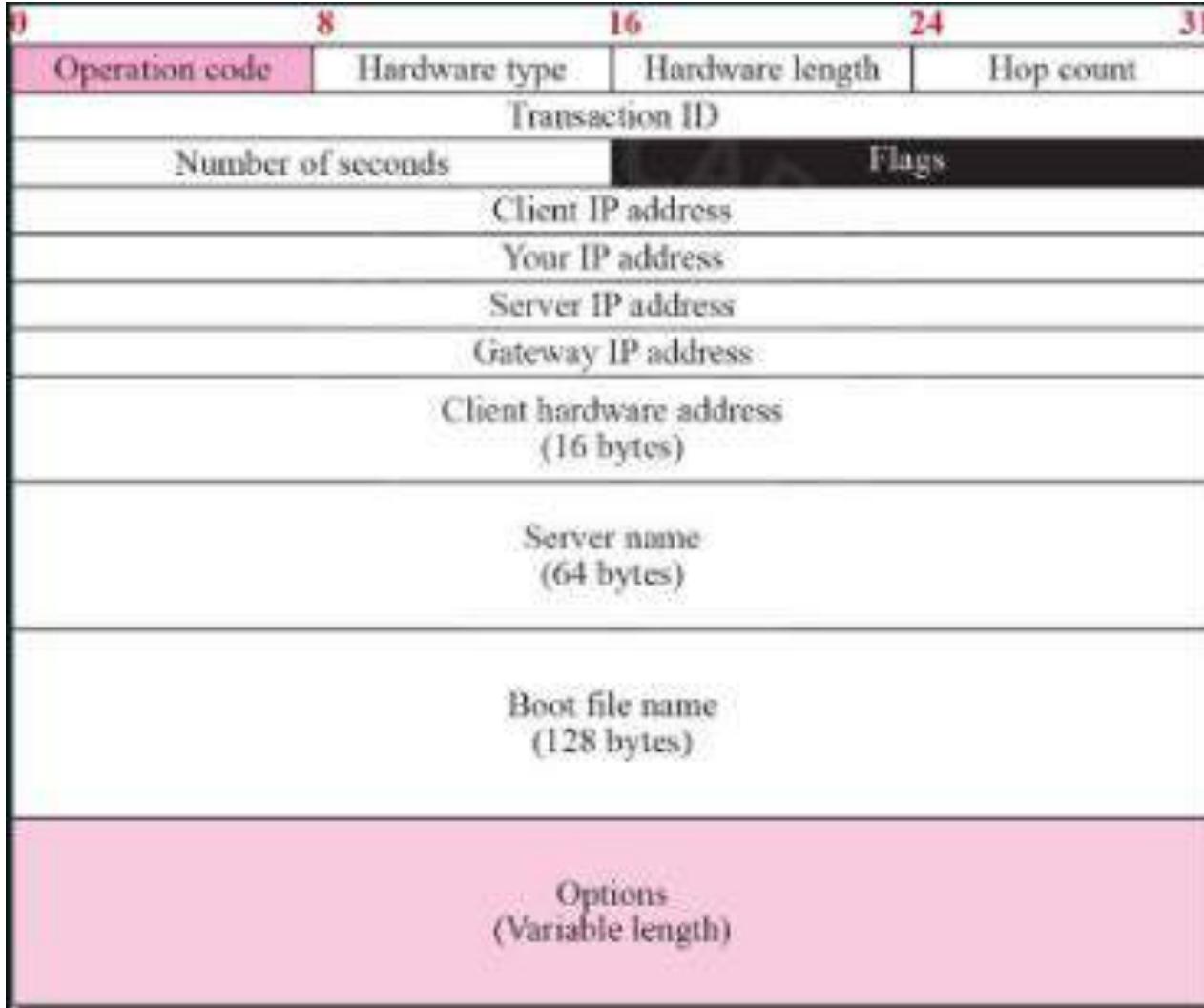
DHCP

❑ *Dynamic Host Configuration Protocol .*



DHCP

□ *DHCP Packet Format*



DHCP

DHCP Packet Format

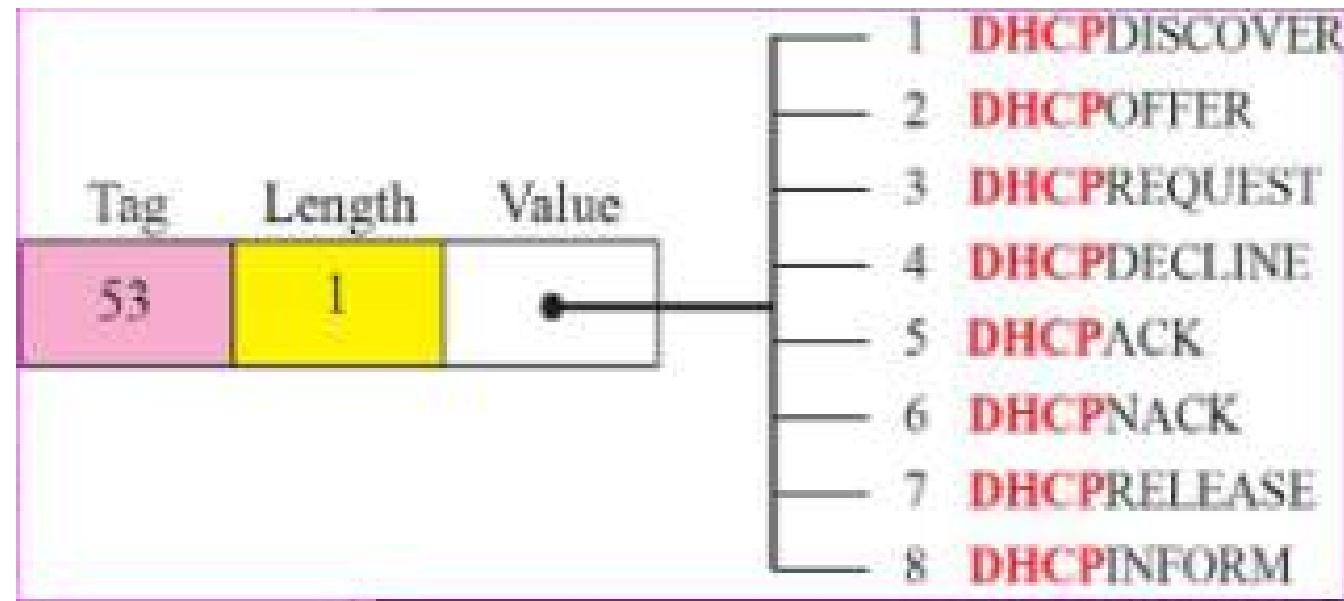
Options for DHCP

Tag	Length	Value	Description	Padding	Tag (0)	End of list	Tag (255)
0			Padding				
1	4	Subnet mask	Subnet mask	Padding			
2	4	Time of the day	Time offset	Other options	Tag	Length	Value (Variable length)
3	Variable	IP addresses	Default router				
4	Variable	IP addresses	Time server				
5	Variable	IP addresses	IEN 16 server				
6	Variable	IP addresses	DNS server				
7	Variable	IP addresses	Log server				
8	Variable	IP addresses	Quote server				
9	Variable	IP addresses	Print server				
10	Variable	IP addresses	Impress				
11	Variable	IP addresses	RLP server				
12	Variable	DNS name	Host name				
13	2	Integer	Boot file size				
53	1	Discussed later	Used for dynamic configuration				
128–254	Variable	Specific information	Vendor specific				
255			End of list				

Length is bytes defined in the length field.

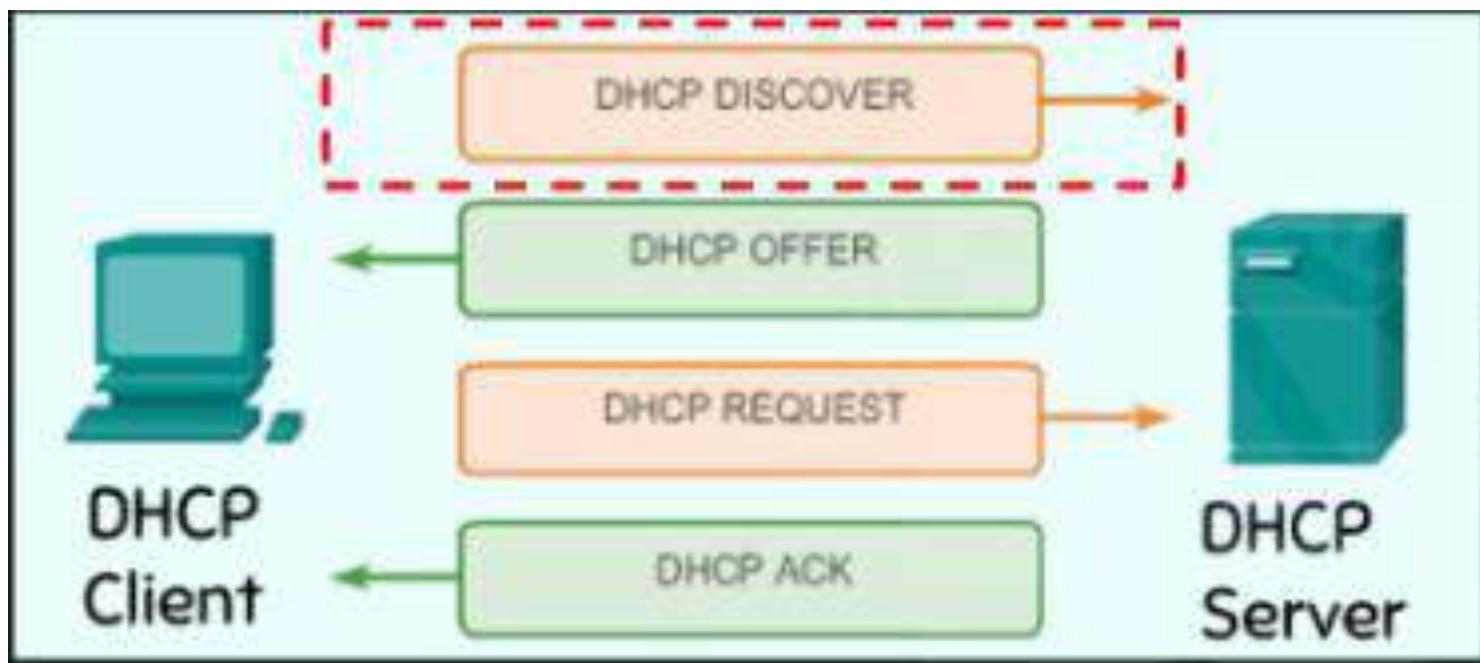
DHCP

□ *DHCP Packet Format*



DHCP

□ *DHCP Operation*



ICMP

□ *Internet Control Message Protocol.*

□ *ICMP is a supporting protocol in the internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating success or failure when communicating with another IP address.*

□ *Example :*

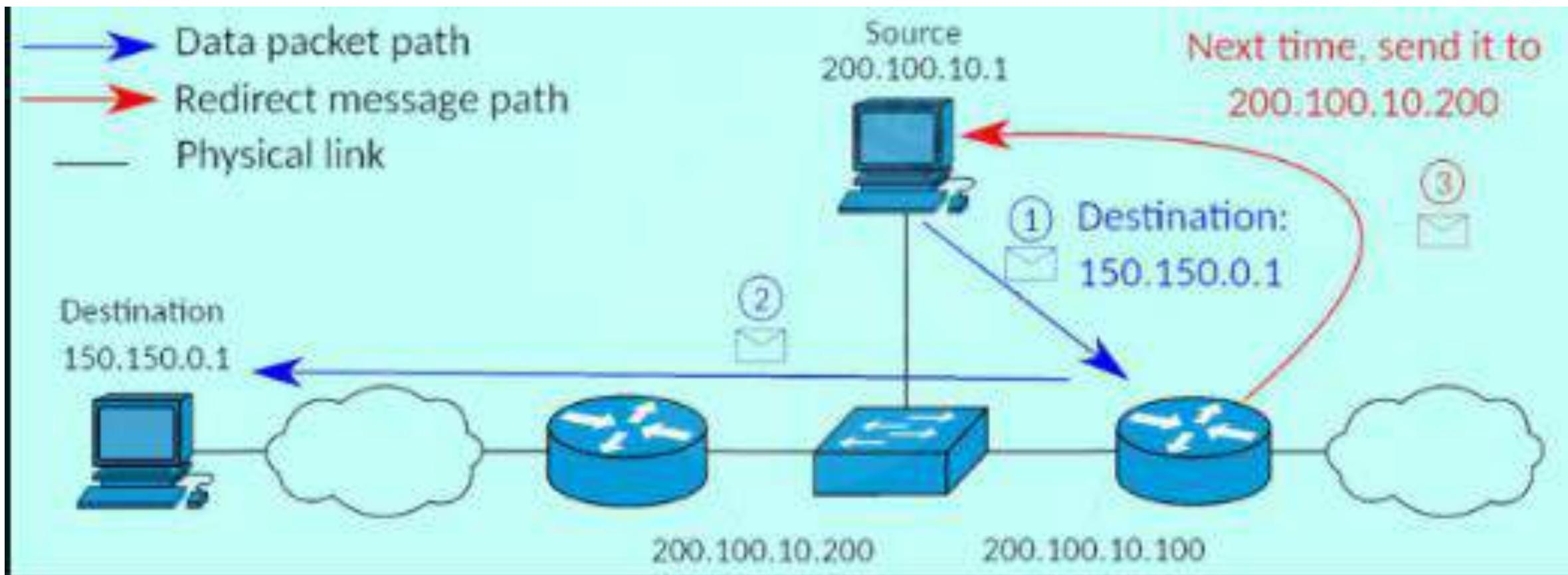
- *Destination host unreachable due to link/node failure*
- *Reassembly process failed*
- *TTL (Time To Live) had reached 0 (So datagram don't cycle forever)*
- *IP header Checksum failed.*

□ *ICMP messages are typically used for diagnostic or control purpose or generated in response to errors in IP operation.*

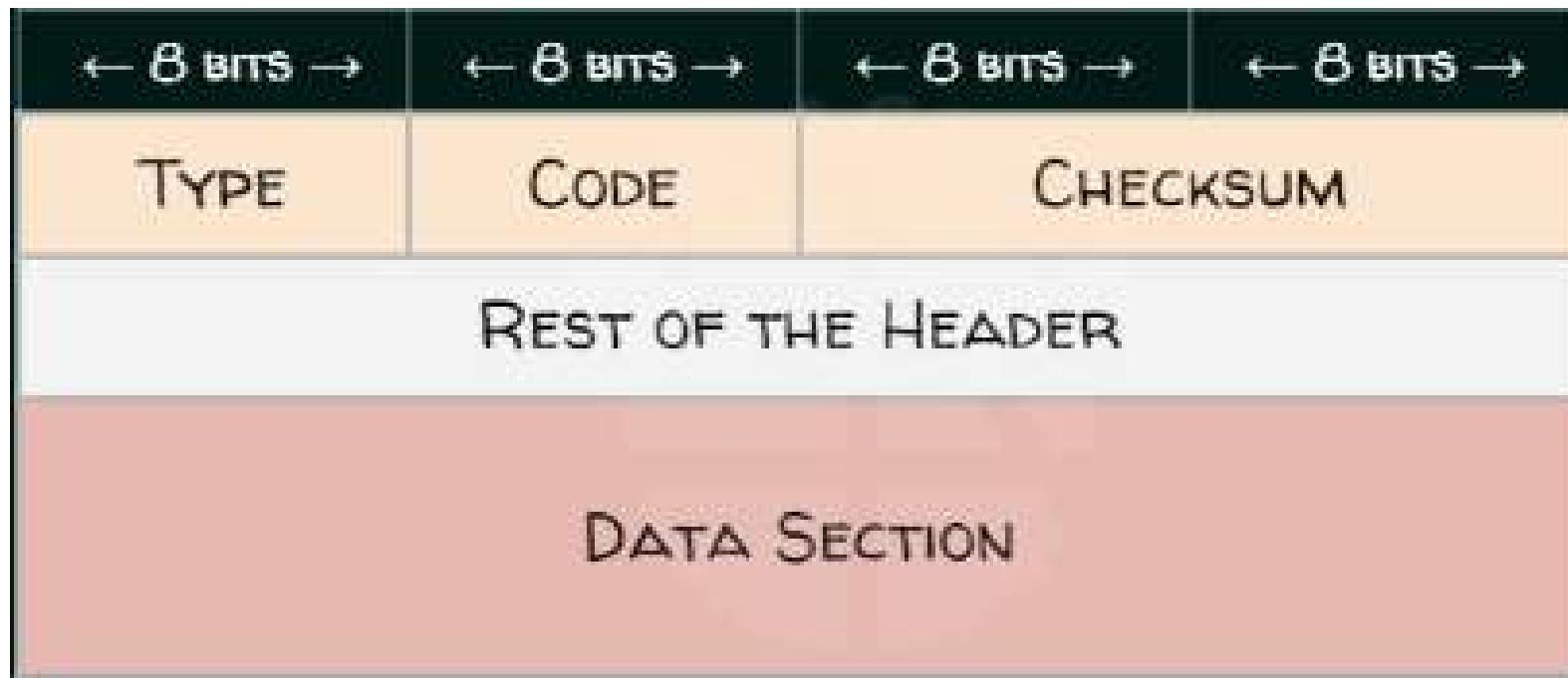
ICMP

- ❑ *ICMP errors are directed to the source IP address of the originating packet*
- ❑ *This protocol defines a collection of error messages that are sent back to the source host whenever a router or host is unable to process an IP packet successfully.*
- ❑ **ICMP redirect**
 - *From router to the source host*
 - *With a better route information*

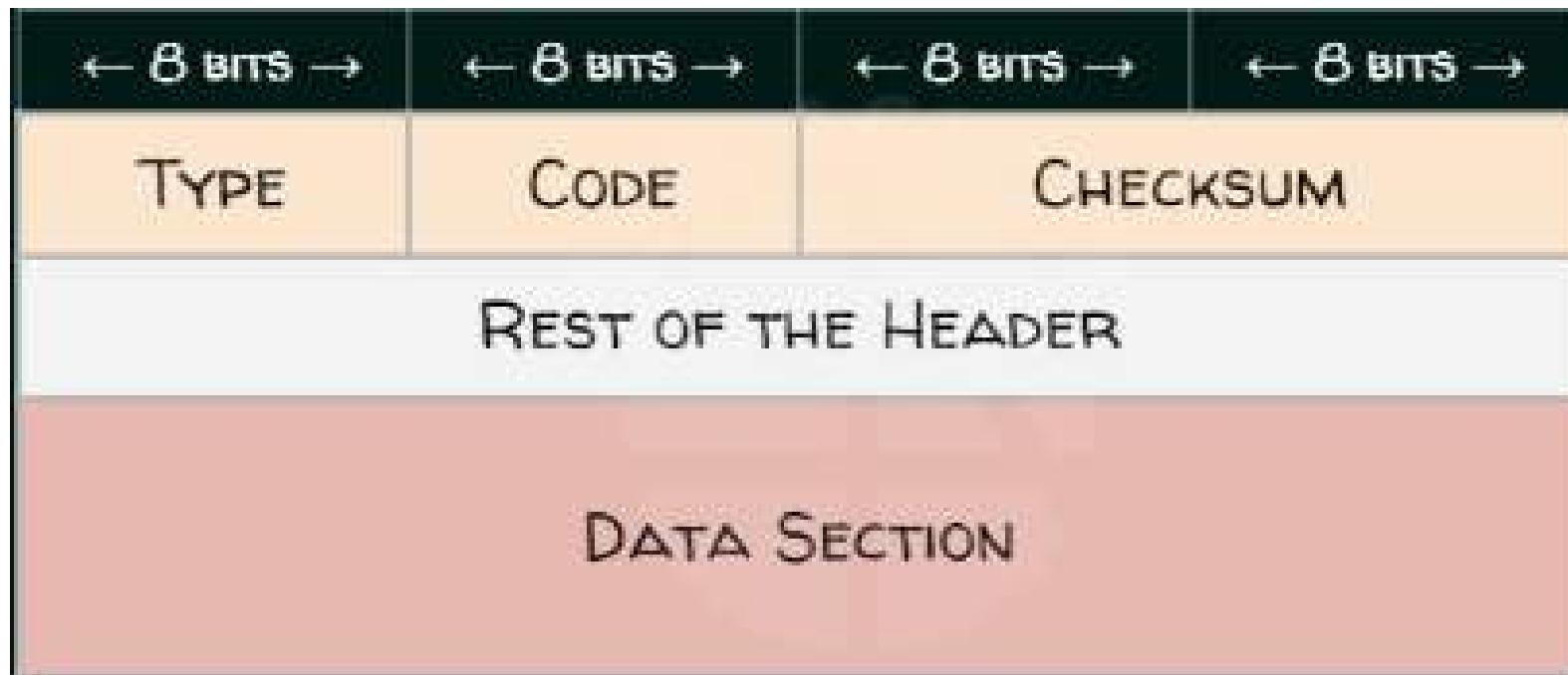
ICMP Redirect



ICMP Packet Format



ICMPv4 Packet Format



ICMPv4 Packet Format

ICMP Parameter Message Format



ICMPv4 Packet Format

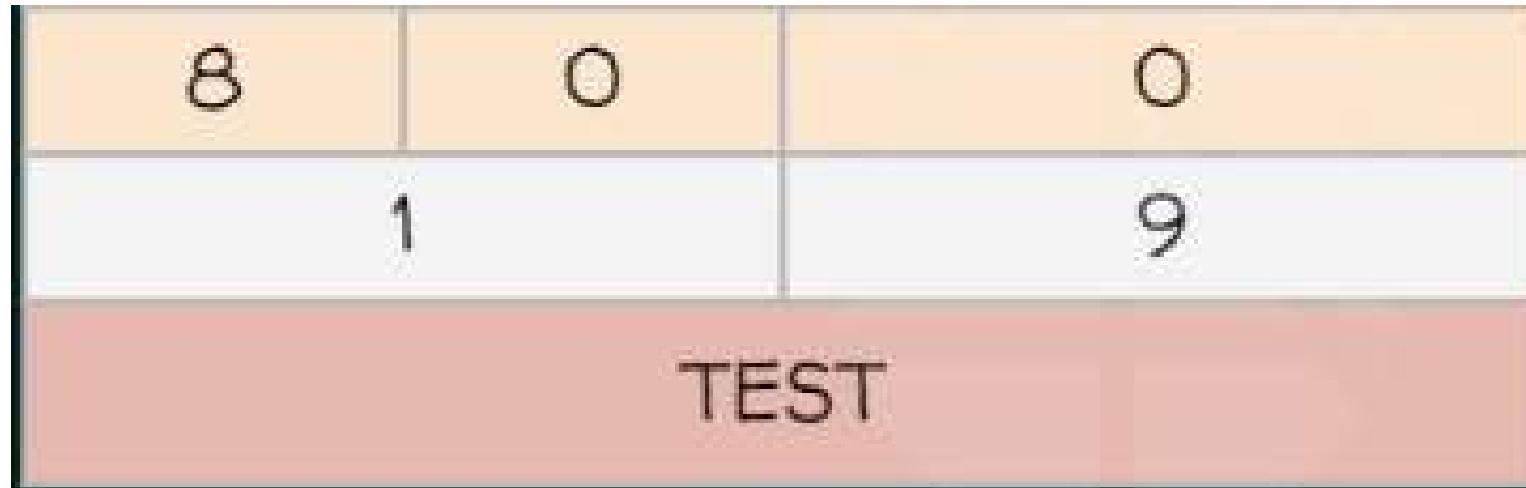
Type	Code	Meaning
0	0	Echo Reply
3	0	Net Unreachable
	1	Host Unreachable
	2	Protocol Unreachable
	3	Port
	4	Frag needed and DF set
	5	Source route failed
	6	Destination network unknown
	7	Destination Host unknown
	8	Source host isolated
	9	
	.	
	13	Communication admin prohibited

ICMPv4 Packet Format

Type	Code	Meaning
4	0	Source Quench
5	0	Redirect data gram from the network
	1	
	2	
	3	
8	0	Echo
9	0	Router advertisement
10	0	Router selection
11	0	TTL exceeded in transit

ICMP

❑ Calculate the checksum for the following ICMPv4 packet

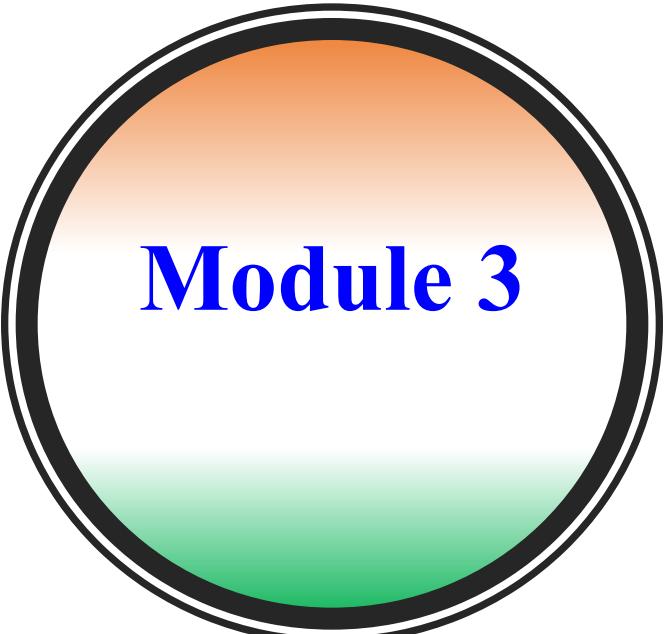


ICMP

IP protocol (Internet Protocol)

- *The responsibility of network layer or Layer 3 is delivery of data from the original source to the destination network.*
- *Service provided by the network layer*
 - Logical addressing
 - Routing





Module 3

Routing Protocol

Various method to build a Routing Table

Static Routing

- A static routing table is created, maintained and updated by a network administrator.
- A static route to every network must be configured on every router for full connectivity.
- This provides a granular level of control over routing, but quickly becomes impractical on large networks.
- Router will not share static routes with each other, thus reducing CPU/RAM overhead and saving bandwidth.

Dynamic Routing

- A dynamic routing table is created , maintained and updated by a routing protocol running on the router.
- The choice of the best route is in the hands of the routing protocol and not the network administrator.
- Example of routing protocols: RIP (Routing Information Protocol, OSPF (Open Shortest Path First) etc.

Various method to build a Routing Table

Static Routing

- However, static routing is not fault tolerant , as any change to the routing infrastructure (such as a link going down, or a new network added) requires manual intervention.
- Routers operating in a purely static environment cannot seamlessly choose a better route if a link becomes unavailable.

Dynamic Routing

- Routers do share dynamic routing information with each other, which increases CPU, RAM and bandwidth usage.
- However, Routing protocols are capable of dynamically choosing a different (or better) path when there is a change to the routing infrastructure.

Various method to build a Routing Table

A static approach has several shortcomings:

- *It does not deal with node or link failures.*
- *It does not consider the addition of new nodes or links.*
- *It implies that edge costs cannot change.*

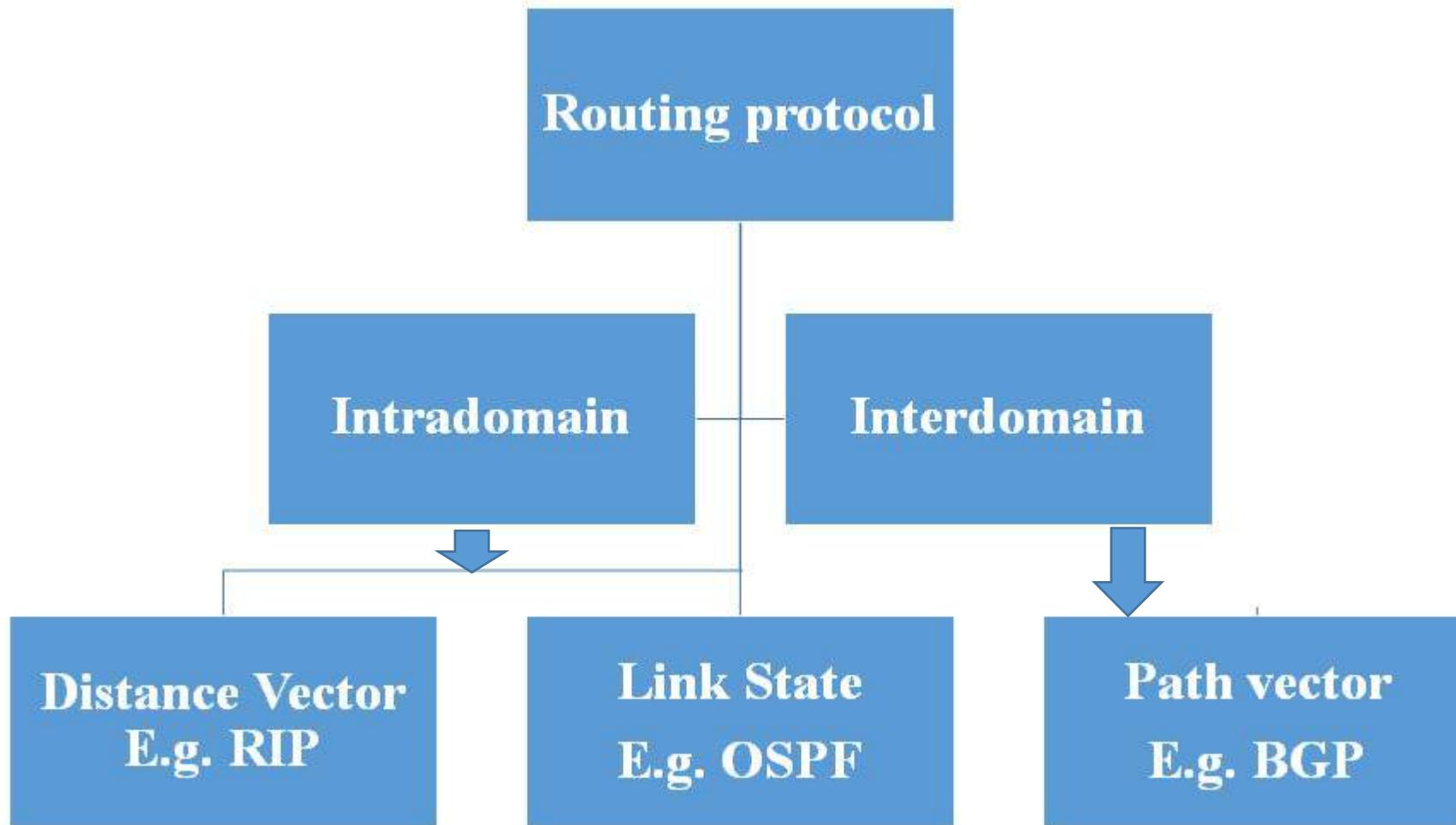
What is the solution?

- *Need a distributed and dynamic protocol*
- ***Two main courses of protocols***
 1. *Distance Vector*
 2. *Link State*

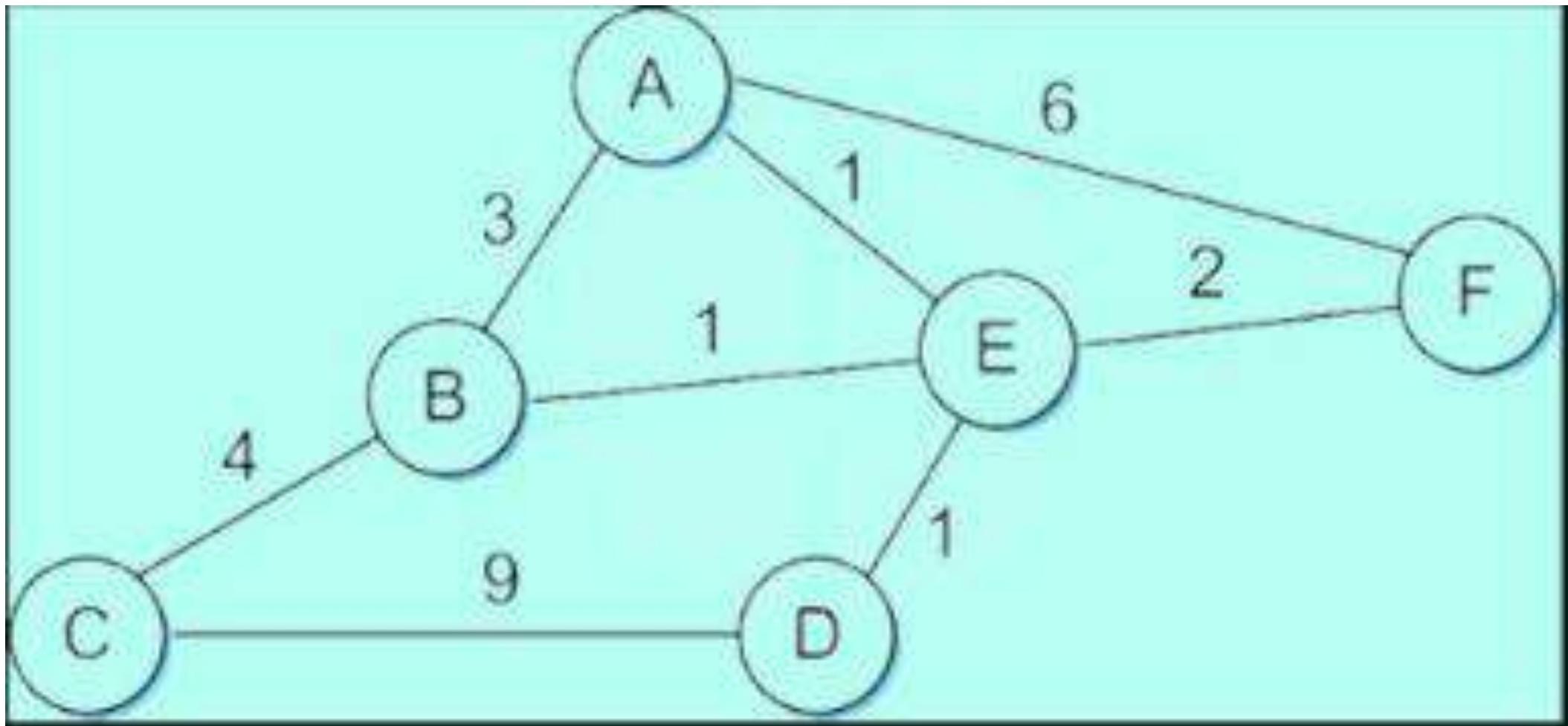
Dynamic Routing Protocols

- *A routing table can be either static and dynamic*
- *A static table is one with manual entries.*
- *A dynamic table is one that is updated automatically when there is a change somewhere in the internet.*
- *A routing protocol is a combination of rules and procedures that lets router in the internet inform each other of changes.*

Popular Routing Protocols

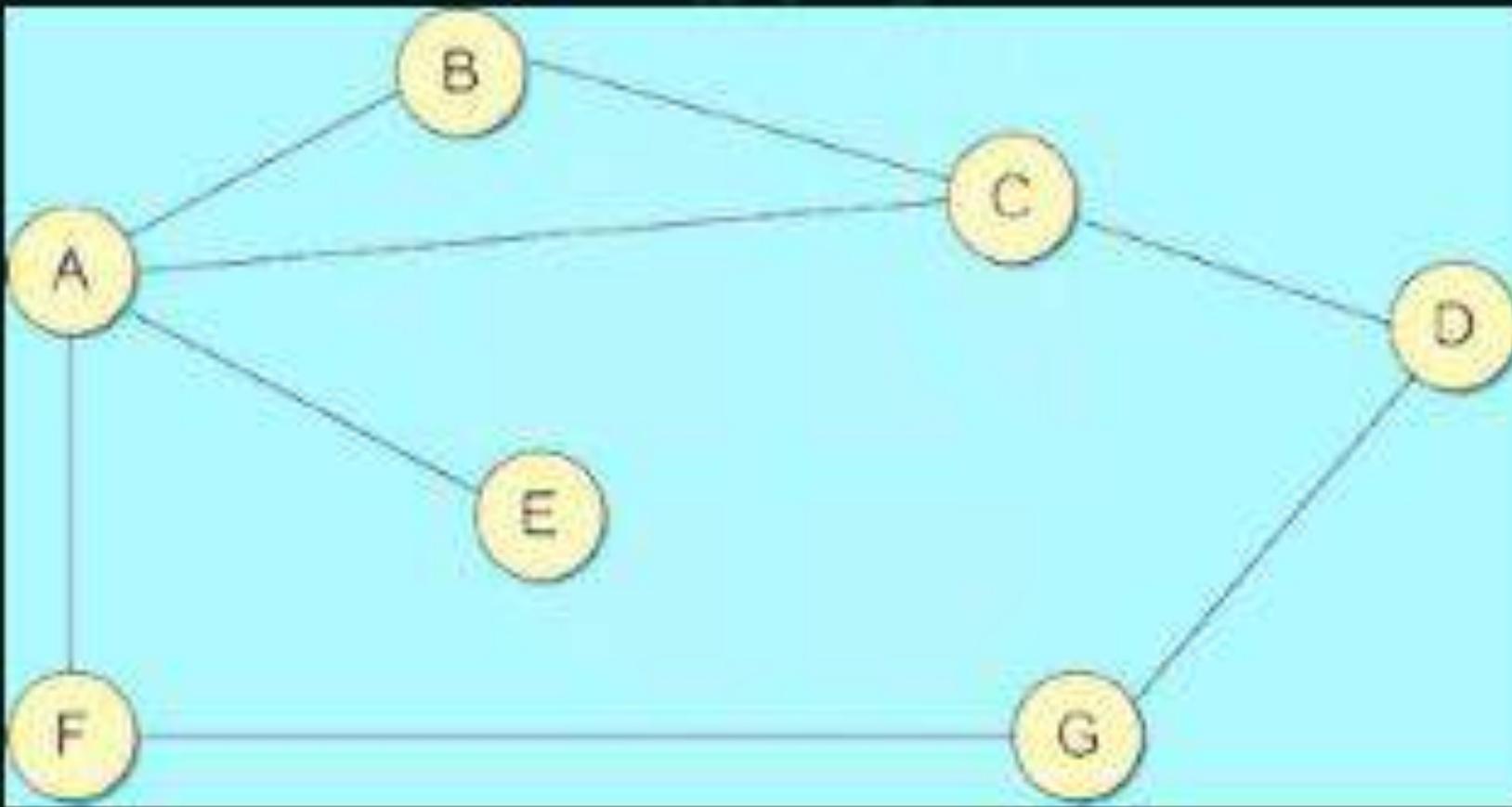


Network as a graph



Distance Vector Routing

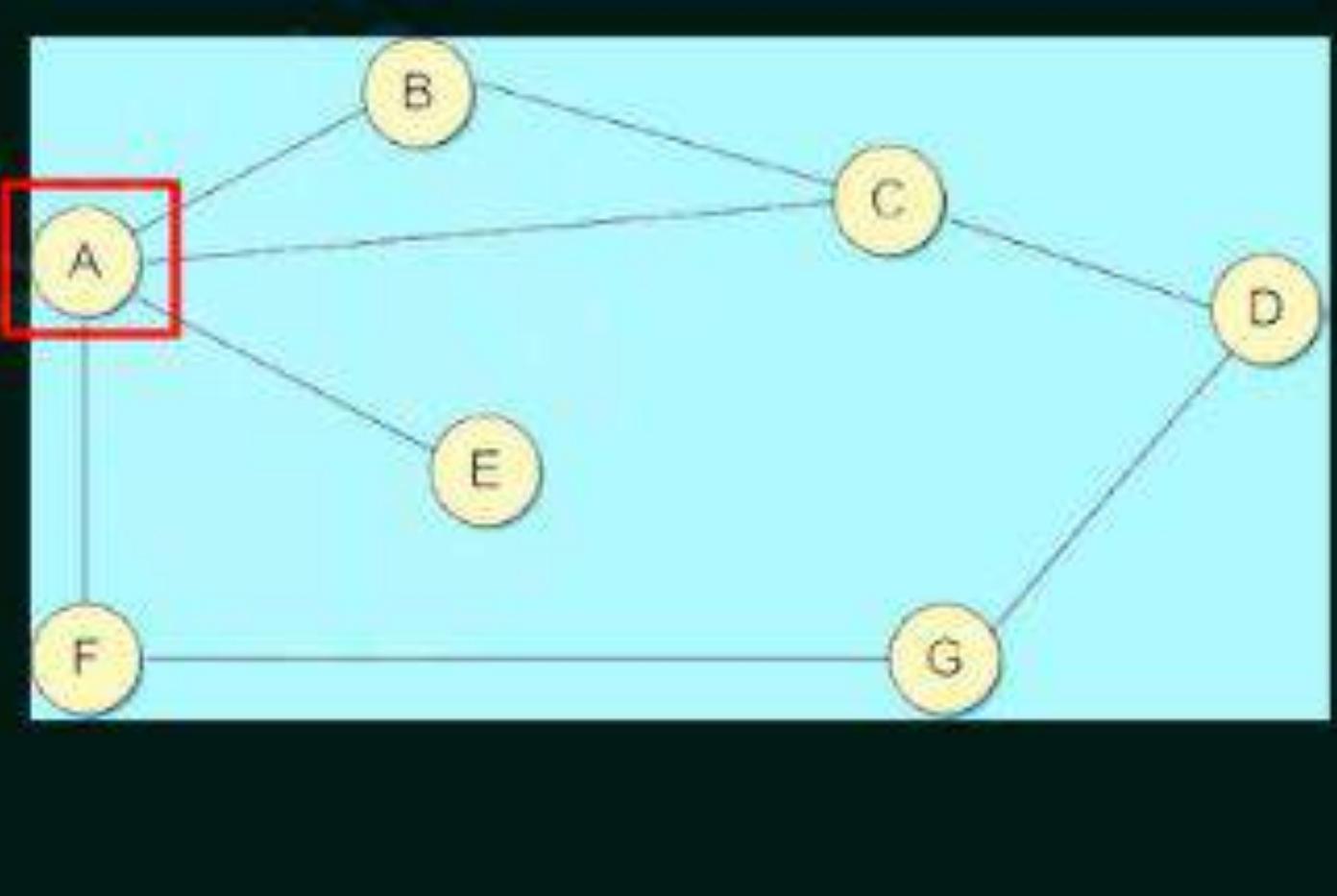
- *Each node construct a one dimensional array (a vector) containing the distances (costs) to all other nodes and distributes that vector to its immediate neighbours.*
- *Starting assumption is that each node knows the cost of the link to each of its directly connected neighbours i.e. the immediate neighbours.*
- *The distance vector routing algorithm is sometimes called as Bellman-Ford algorithm.*
- *Every T seconds each router sends its table to its neighbour and each router then updates its table based on the new information.*
- *Problem includes fast response to good news and slow response to bad news.*
- *Also too many messages to update.*



Routing Table Entries: (Destination, Distance/Cost, Next Hop)
Node A: (B,1,B), (C,1,C), (F,1,F), (E,1,E), (D,2,C) etc.,

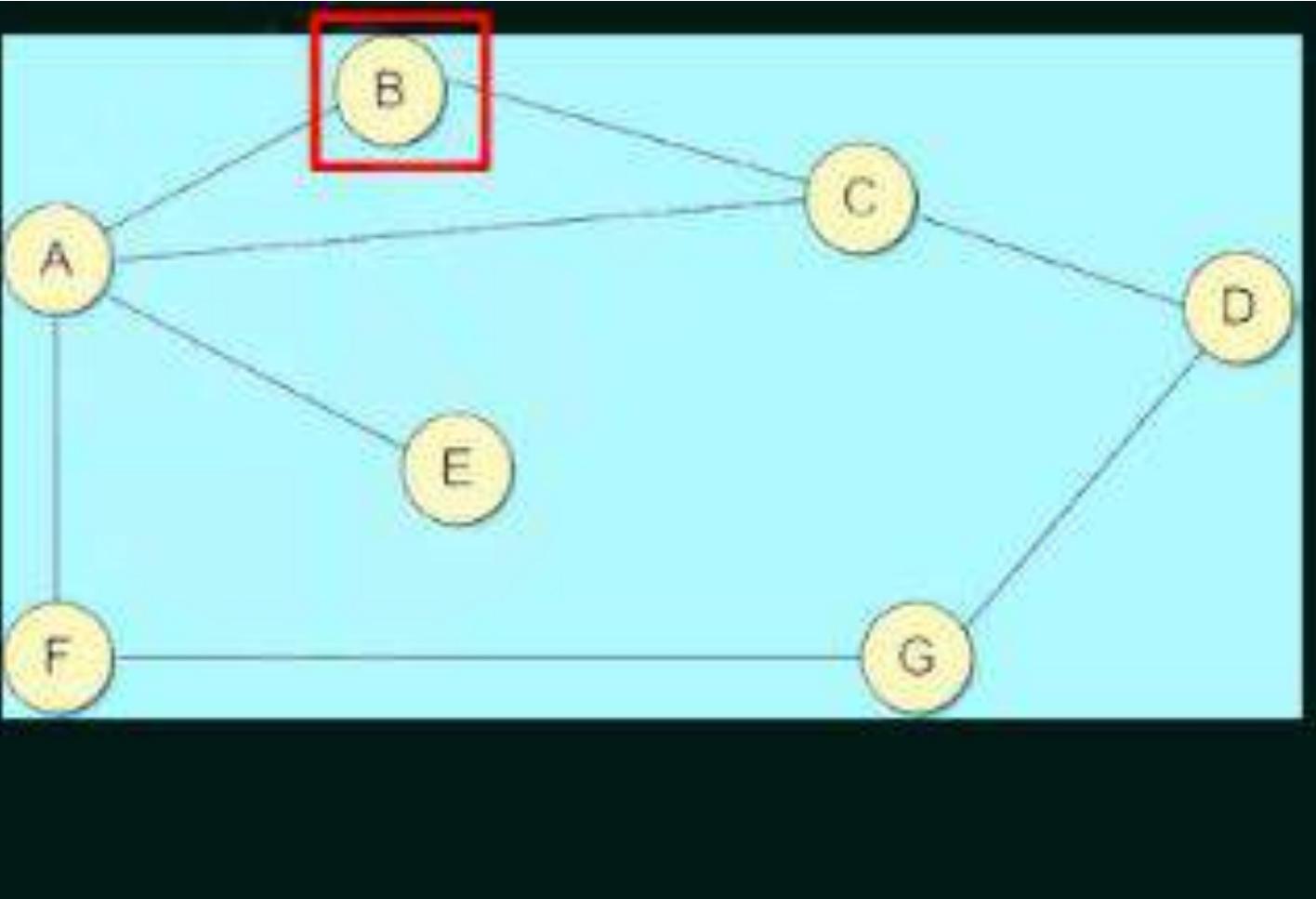
Initial Routing Table of A

Destination	Cost	Next Hop
A	0	-
B	1	B
C	1	C
D	∞	-
E	1	E
F	1	F
G	∞	-



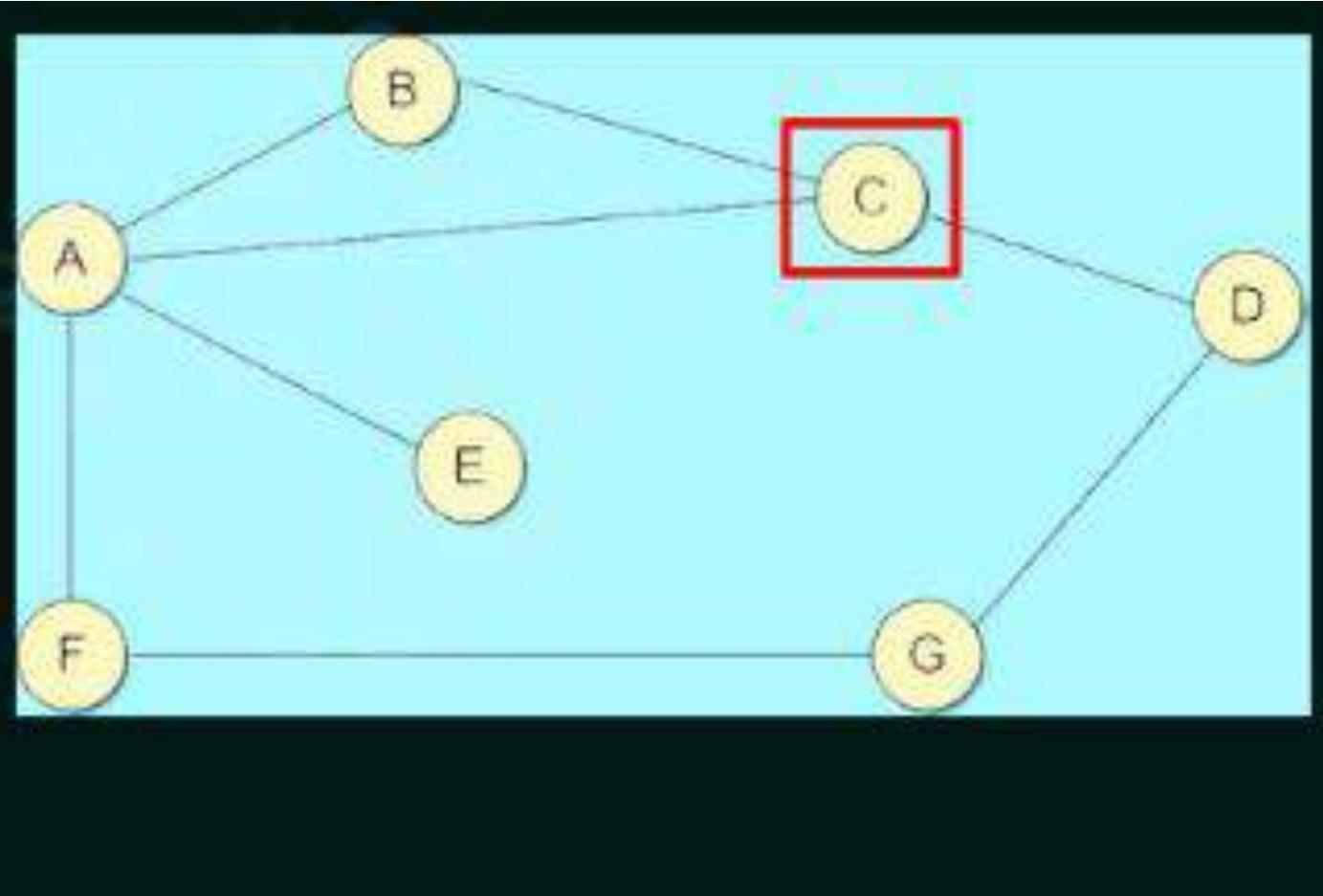
Initial Routing Table of B

Destination	Cost	Next Hop
A	1	A
B	0	-
C	1	C
D	∞	-
E	∞	-
F	∞	-
G	∞	-



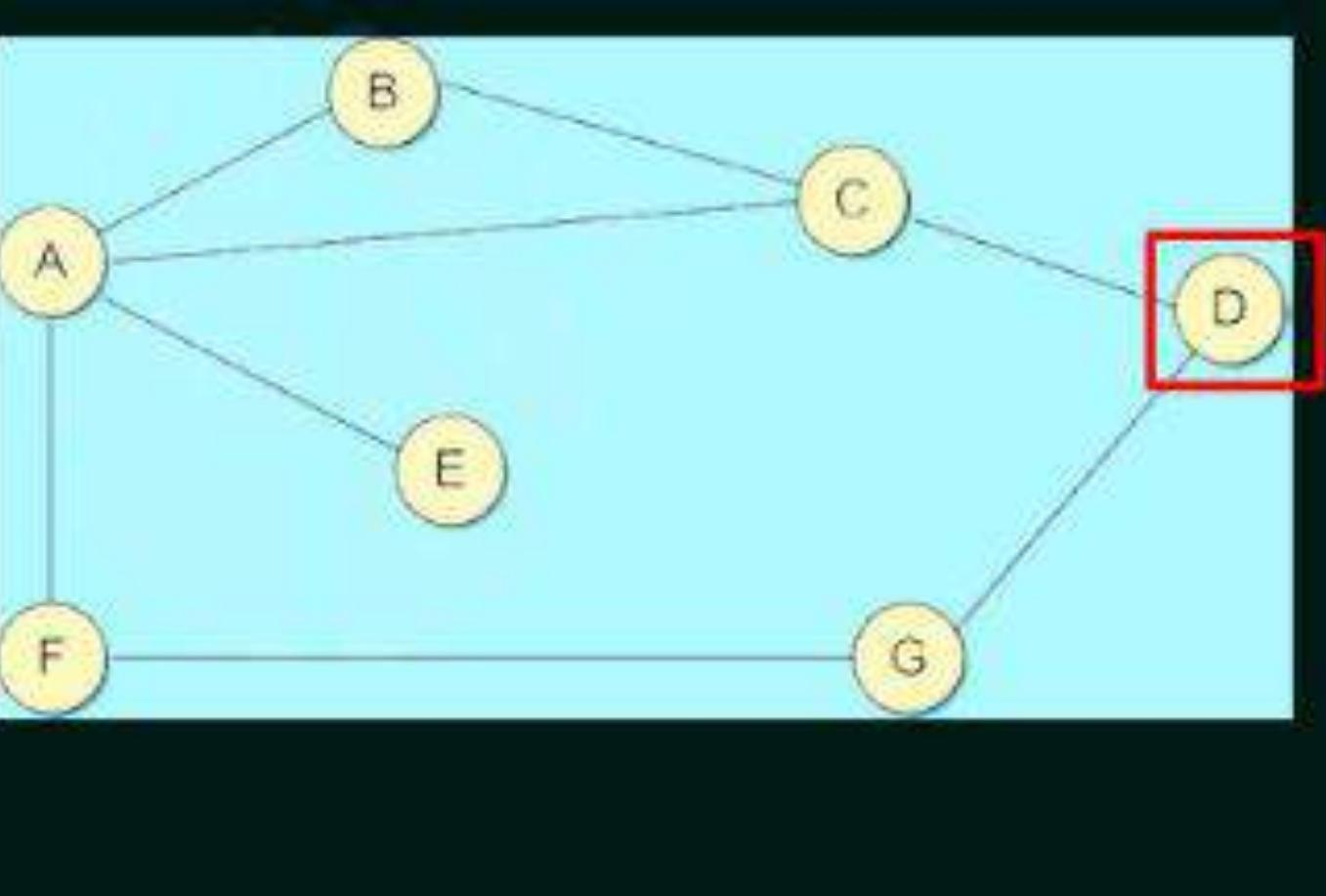
Initial Routing Table of C

Destination	Cost	Next Hop
A	1	A
B	1	B
C	0	-
D	1	D
E	∞	-
F	∞	-
G	∞	-



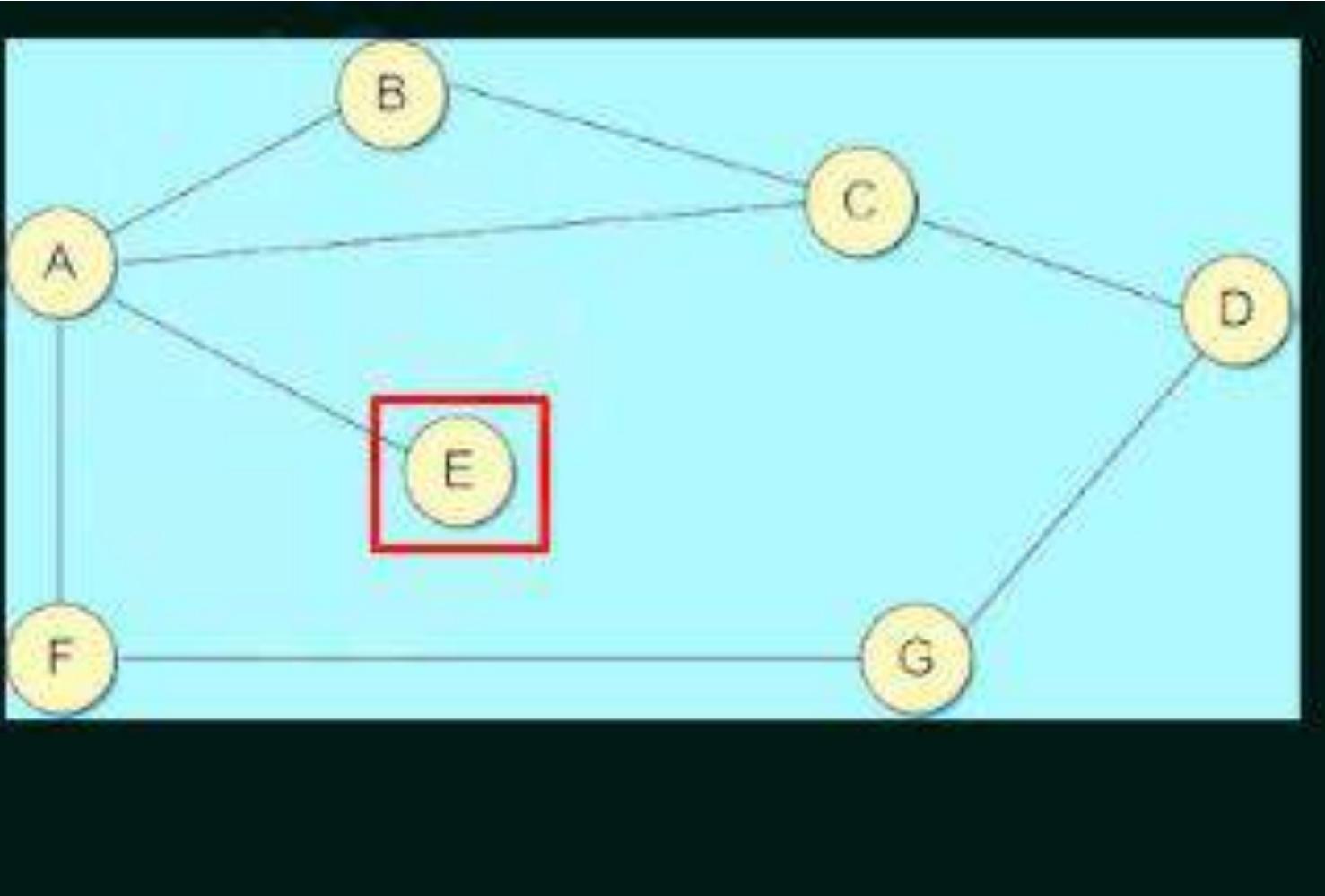
Initial Routing Table of D

Destination	Cost	Next Hop
A	∞	-
B	∞	-
C	1	C
D	0	-
E	∞	-
F	∞	-
G	1	G



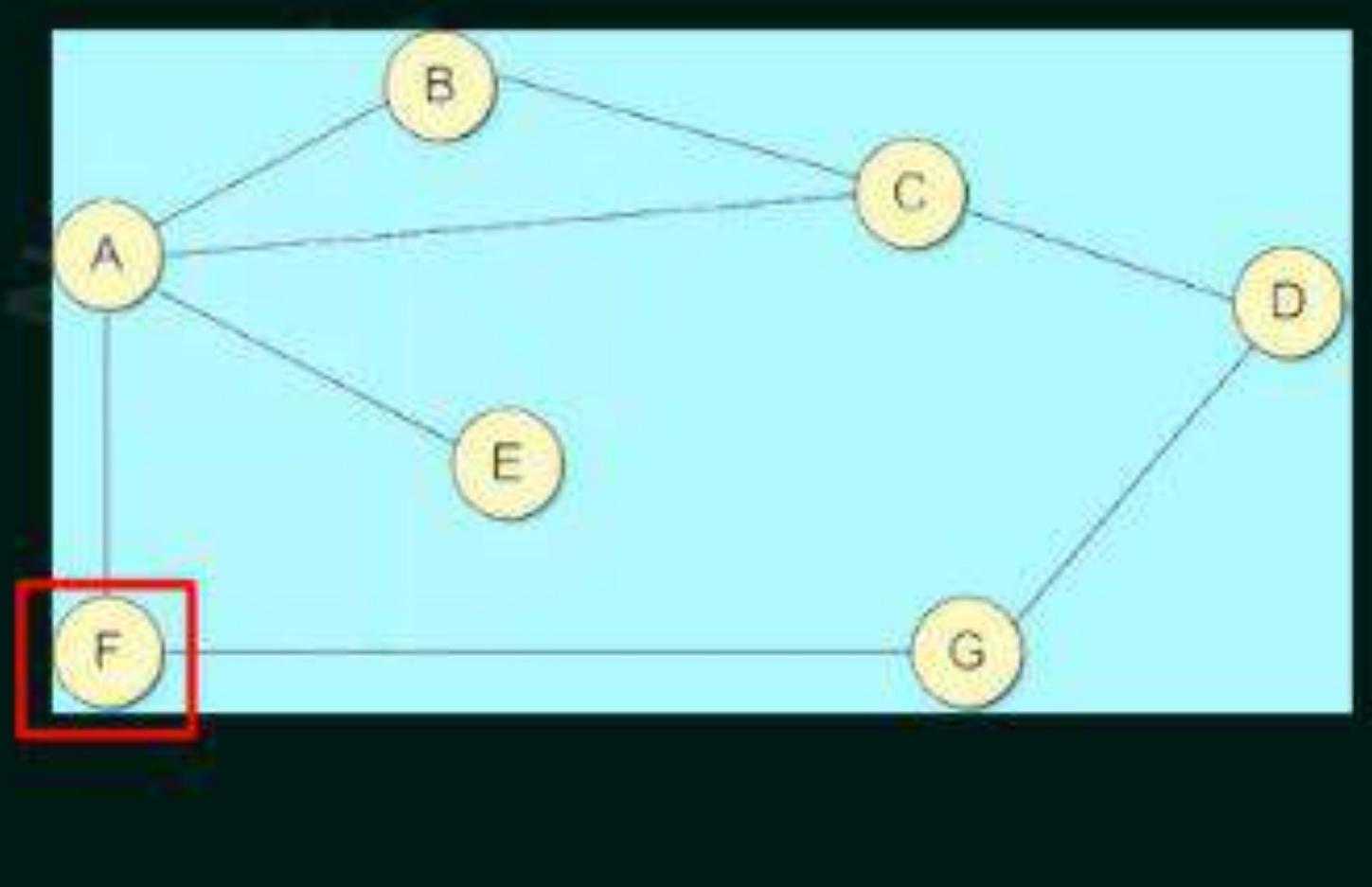
Initial Routing Table of E

Destination	Cost	Next Hop
A	1	A
B	∞	-
C	∞	-
D	∞	-
E	0	-
F	∞	-
G	∞	-



Initial Routing Table of F

Destination	Cost	Next Hop
A	1	A
B	∞	-
C	∞	-
D	∞	-
E	∞	-
F	0	-
G	1	G



Initial Routing Table of G

Destination	Cost	Next Hop
A	∞	-
B	∞	-
C	∞	-
D	1	1
E	∞	-
F	1	1
G	0	-

```
graph TD; A((A)) --- B((B)); A --- C((C)); A --- D((D)); A --- E((E)); A --- F((F)); G((G)) --- F; G --- D; G --- C;
```

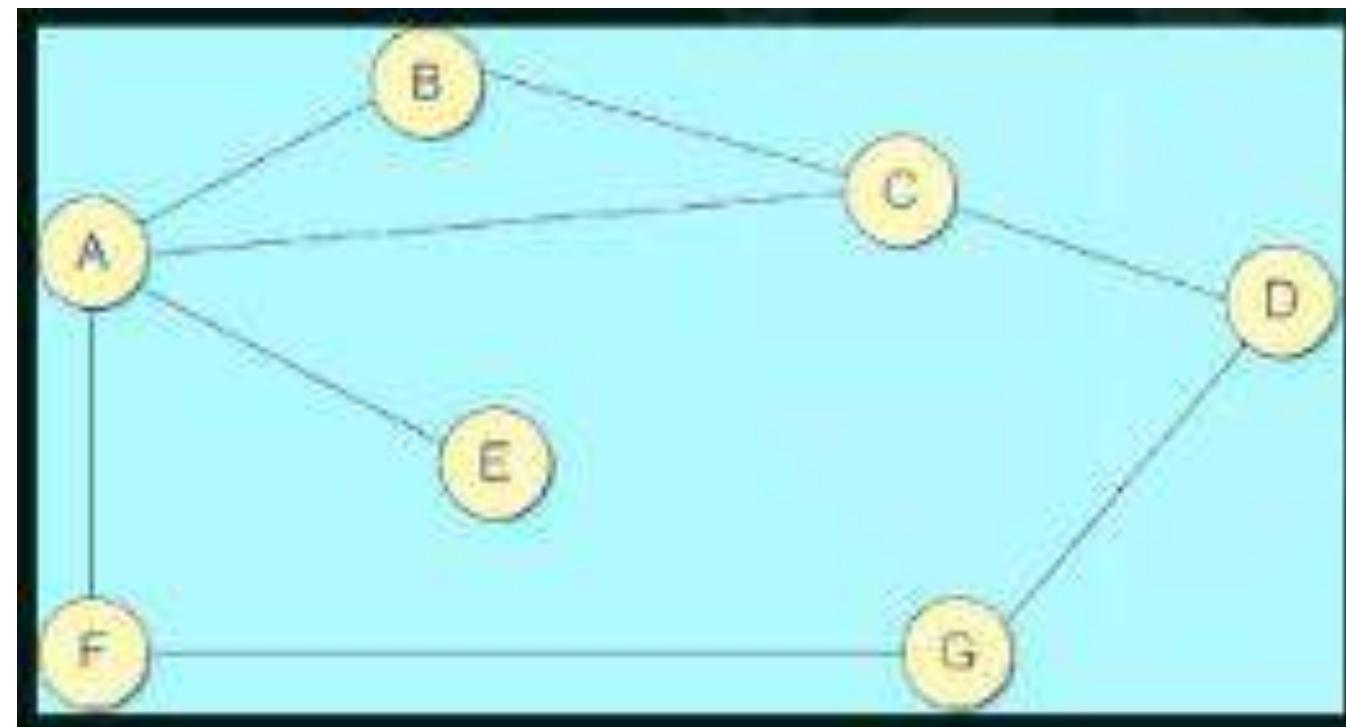
Initial Distance Vector stored at Each Node

Information stored at Node	Distance to reach node						
	A	B	C	D	E	F	G
A	0	1	1	∞	1	1	∞
B	1	0	1	∞	∞	∞	∞
C	1	1	0	1	∞	∞	∞
D	∞	∞	1	0	∞	∞	1
E	1	∞	∞	∞	0	∞	∞
F	1	∞	∞	∞	∞	0	1
G	∞	∞	∞	1	∞	1	0

Exchange of Routing table at A from directly connected Neighbours

A	
A	0
B	1
C	1
D	∞
E	1
F	1
G	∞

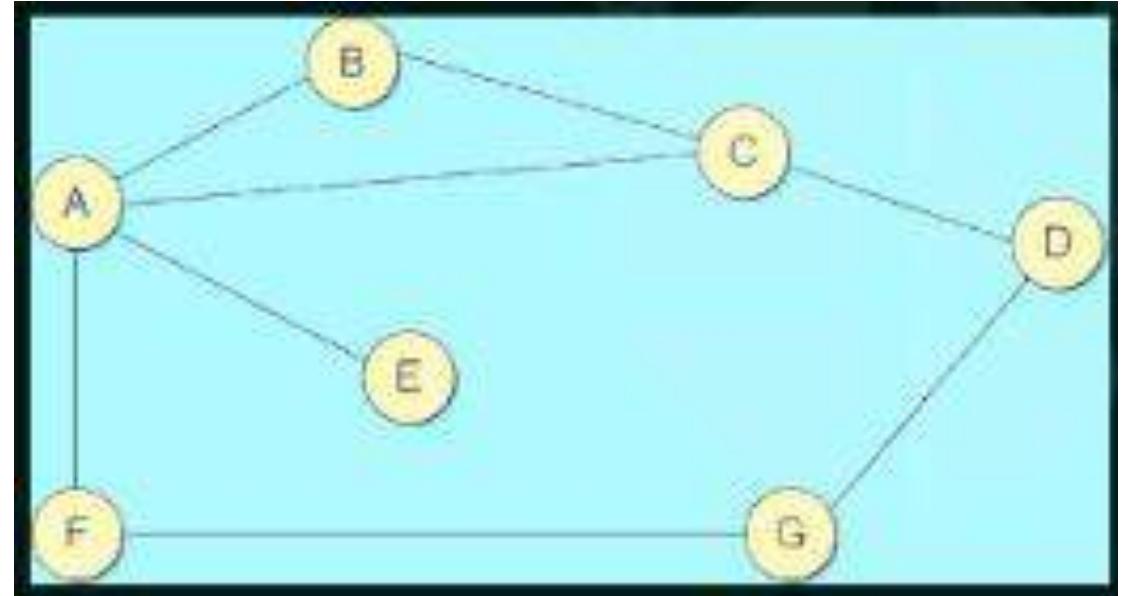
B	
A	1
B	0
C	1
D	∞
E	∞
F	∞
G	∞



Exchange of Routing table at A from directly connected Neighbours

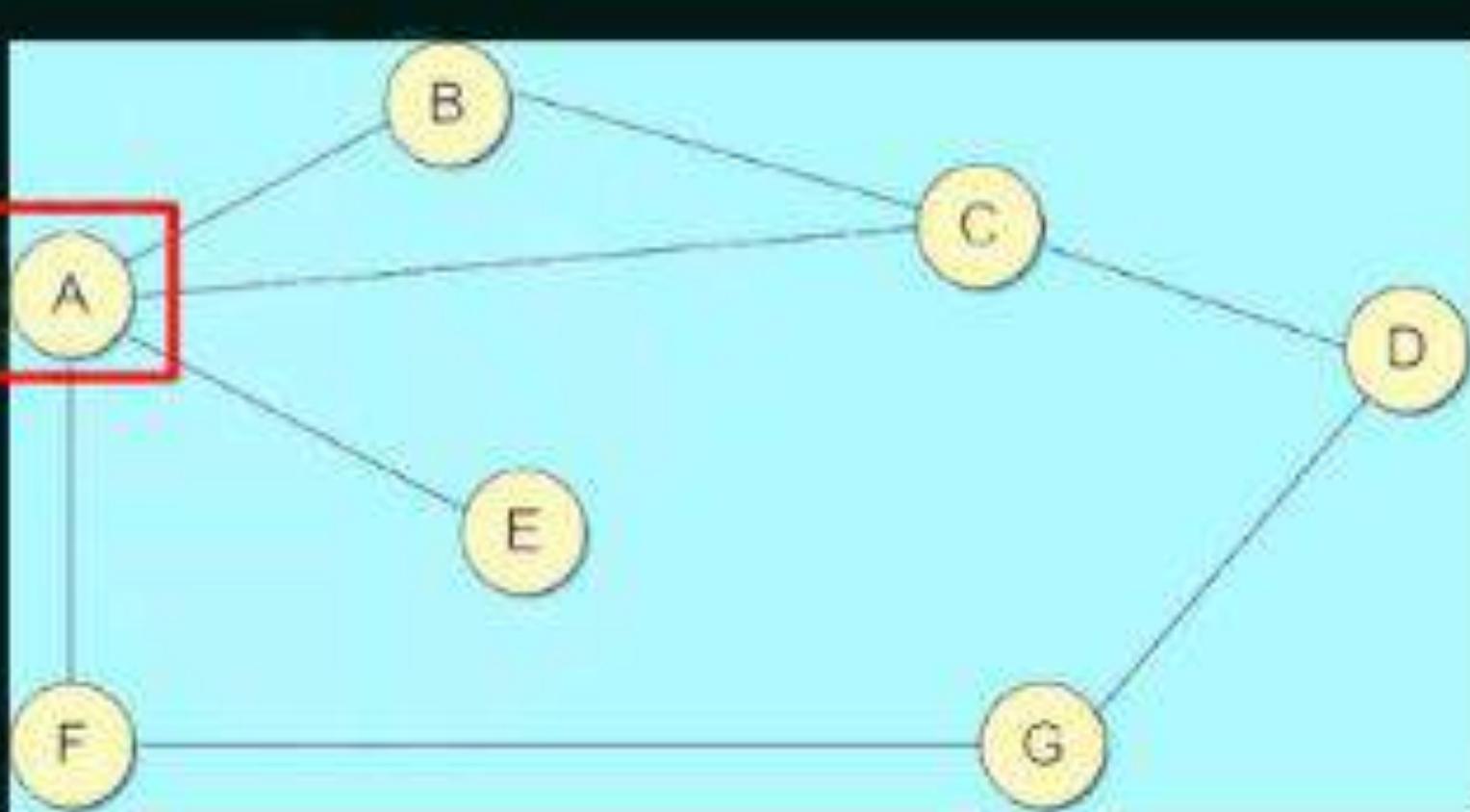
C	A	B	C	D	E	F	G
A	1						
B	1						
C	0						
D	1						
E	∞						
F	∞						
G	∞						

F	
A	1
B	∞
C	∞
D	∞
E	∞
F	0
G	1



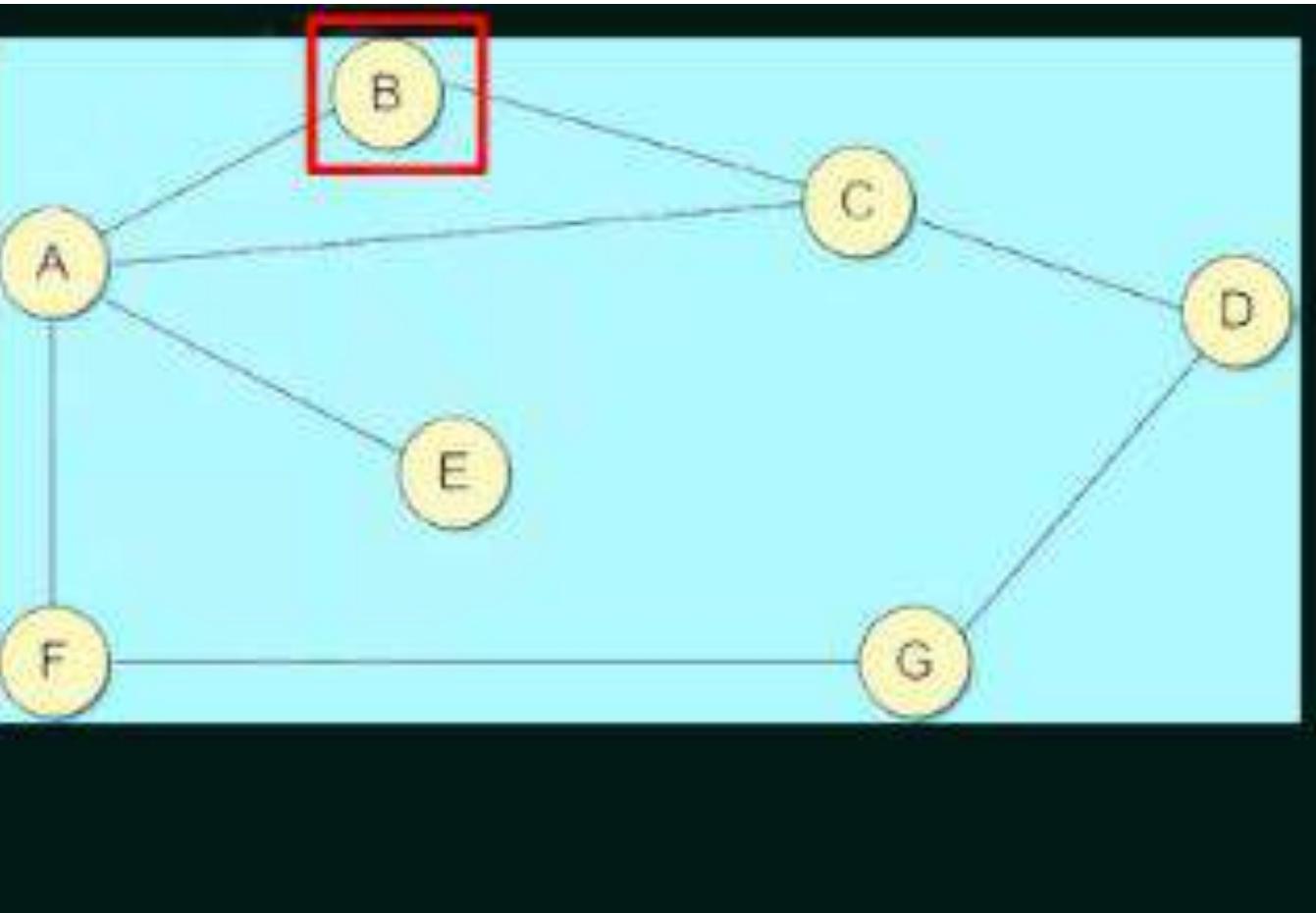
Final routing Table at A

Destination	Cost	Next Hop
A	0	-
B	1	B
C	1	C
D	2	C
E	1	E
F	1	F
G	2	F



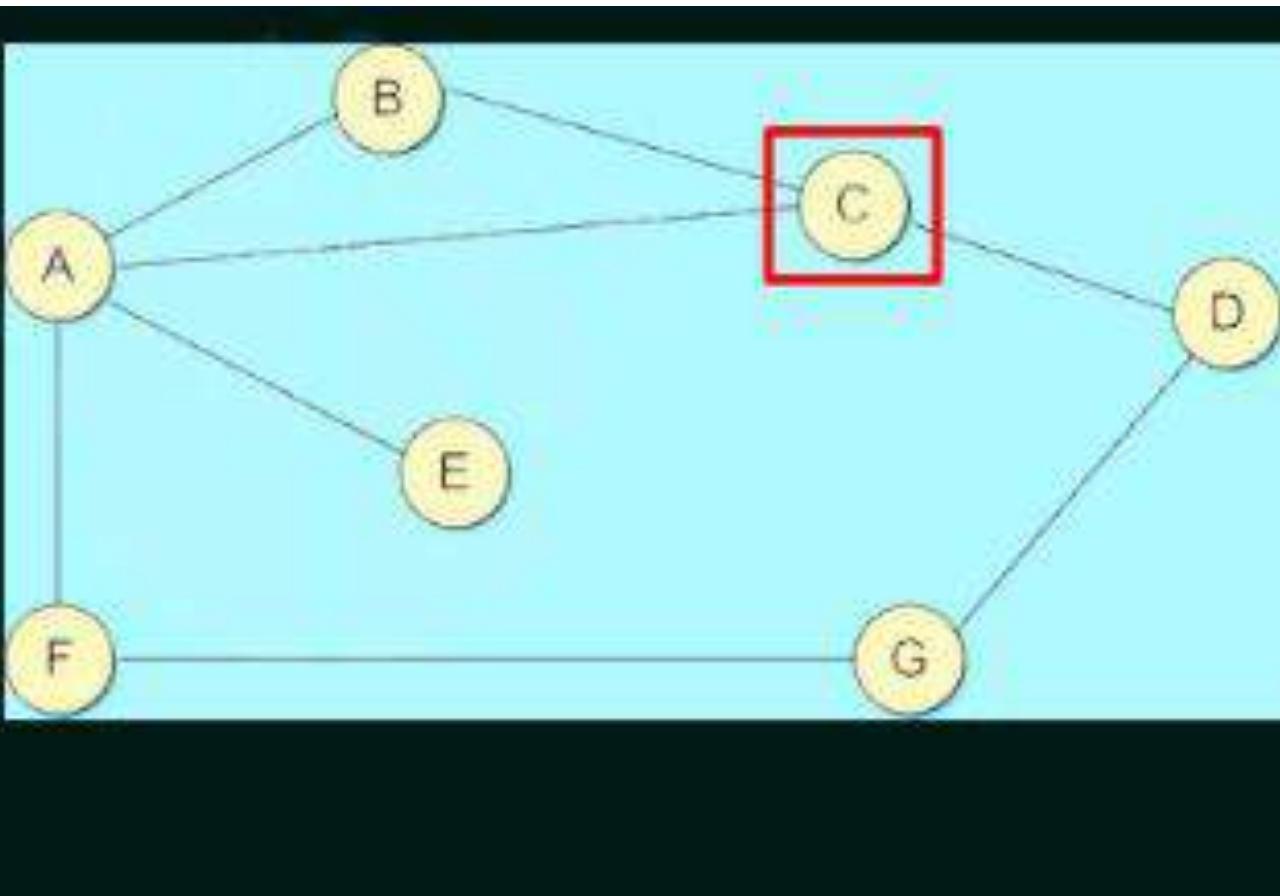
Final routing Table at B

Destination	Cost	Next Hop
A	1	A
B	0	-
C	1	C
D	2	C
E	2	A
F	2	F
G	3	F

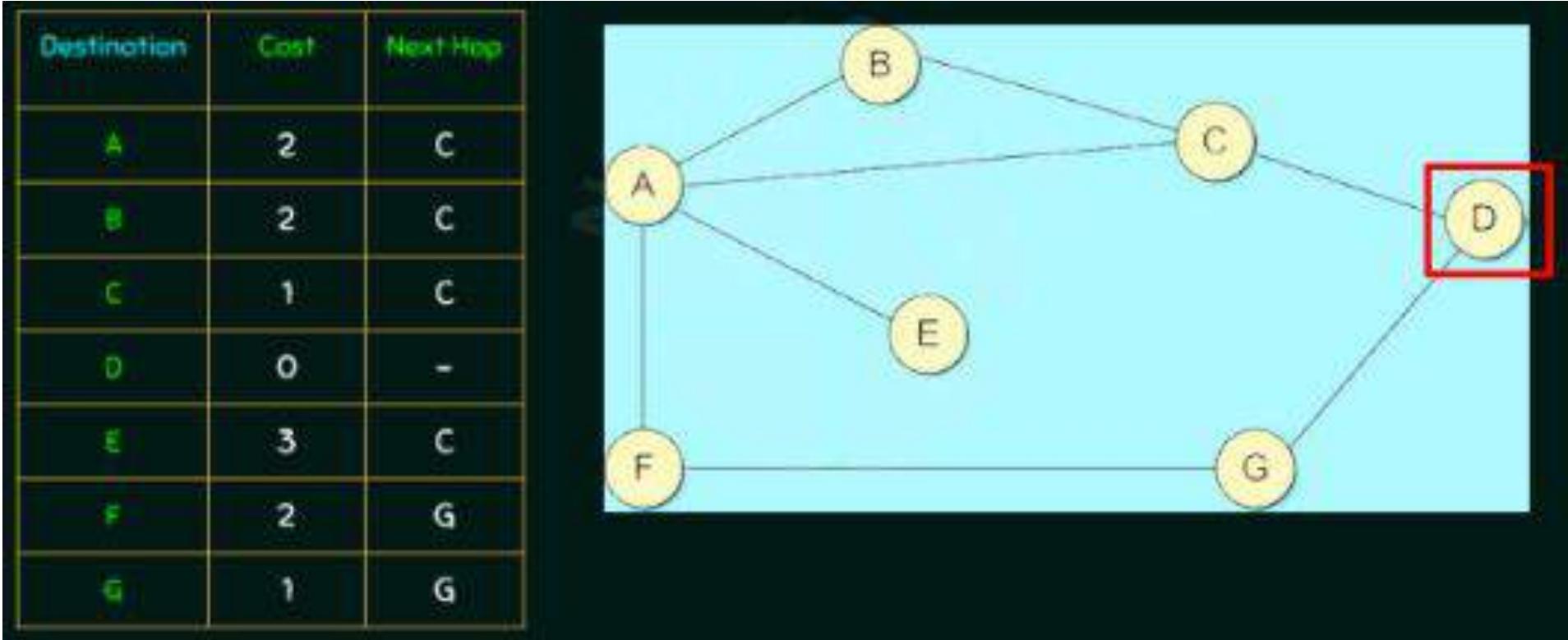


Final routing Table at C

Destination	Cost	Next Hop
A	1	A
B	1	B
C	0	-
D	1	D
E	2	A
F	2	A
G	2	D

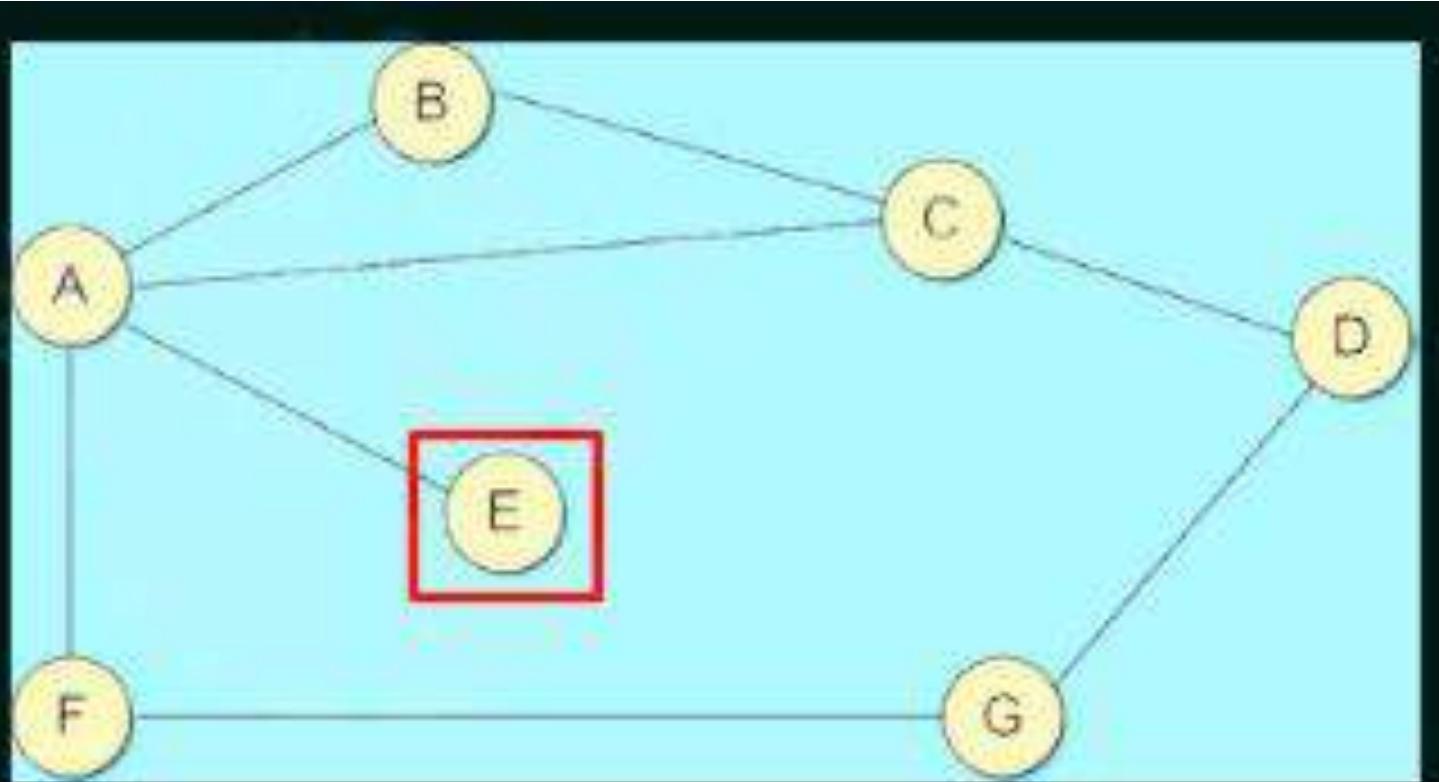


Final routing Table at D



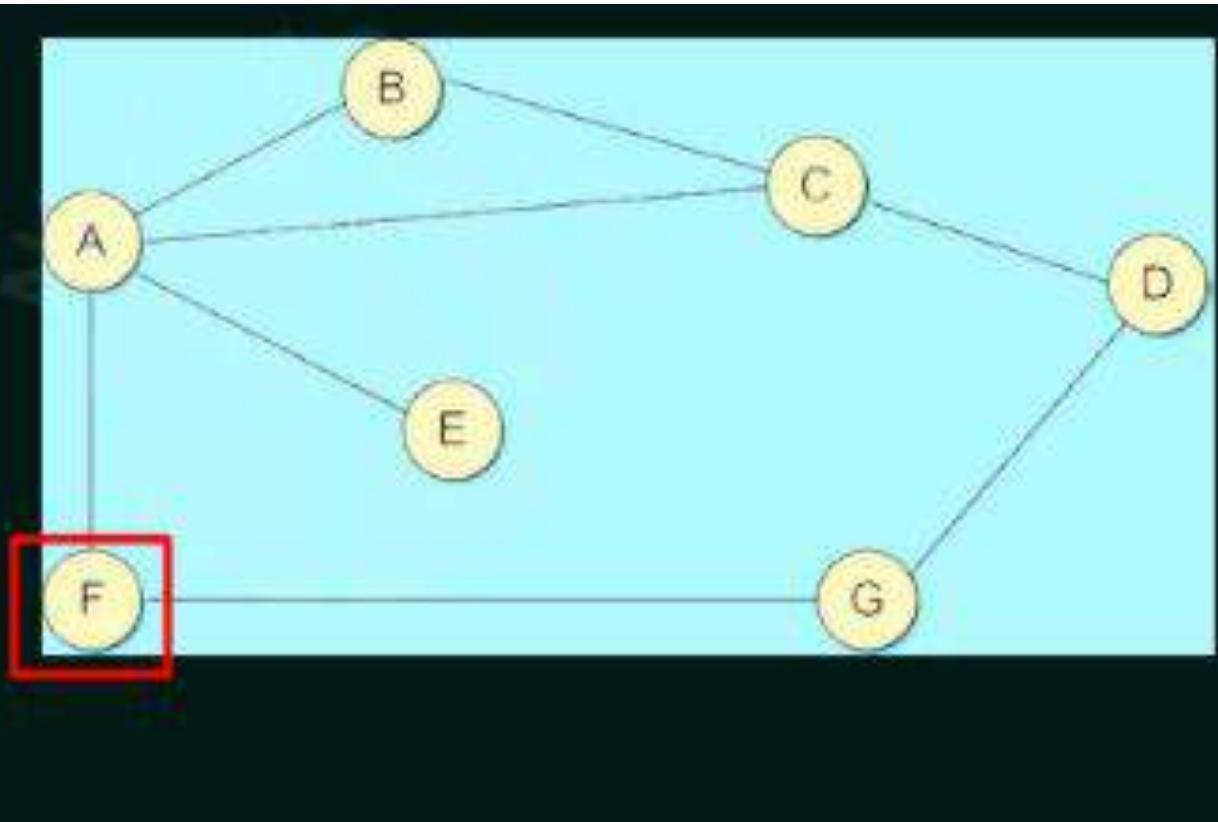
Final routing Table at E

Destination	Cost	Next Hop
A	1	A
B	2	A
C	2	A
D	3	A
E	0	-
F	2	A
G	3	A



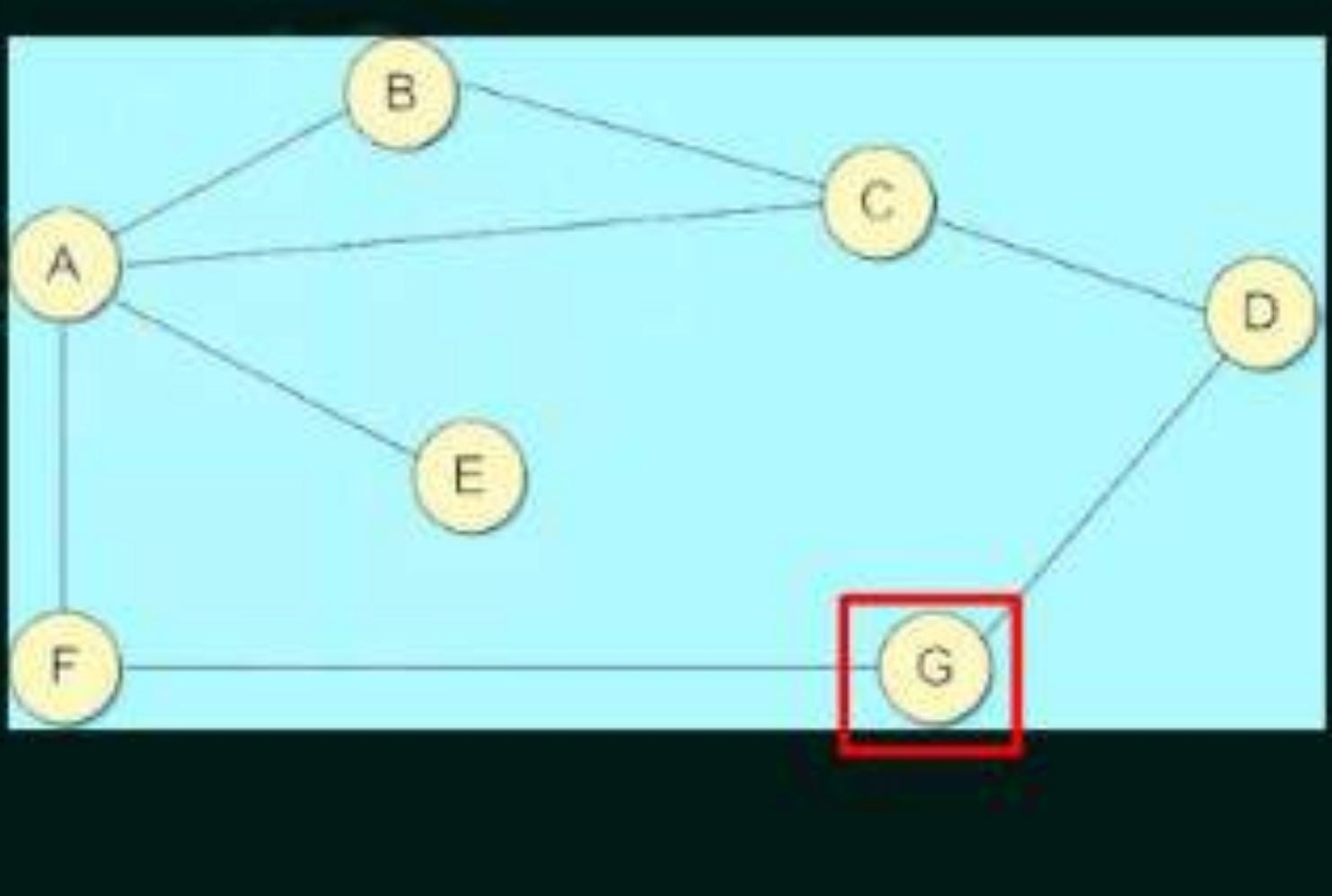
Final routing Table at F

Destination	Cost	Next Hop
A	1	A
B	2	A
C	2	A
D	2	G
E	2	A
F	0	-
G	1	G



Final routing Table at G

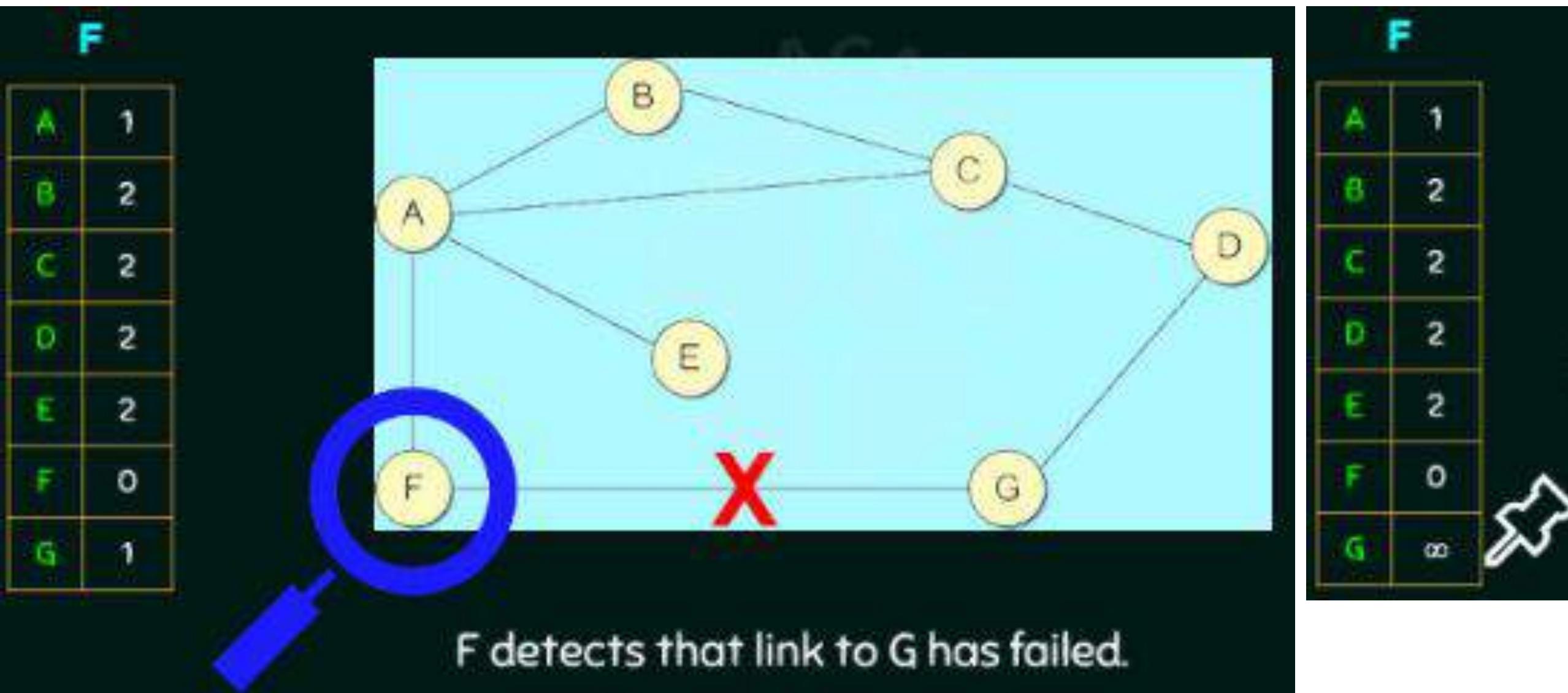
Destination	Cost	Next Hop
A	2	F
B	3	F
C	2	D
D	1	1
E	3	F
F	1	F
G	0	-



Final Distance stored at Each Node

Information stored at Node	Distance to reach node						
	A	B	C	D	E	F	G
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	2	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	2	3	2	1	3	1	0

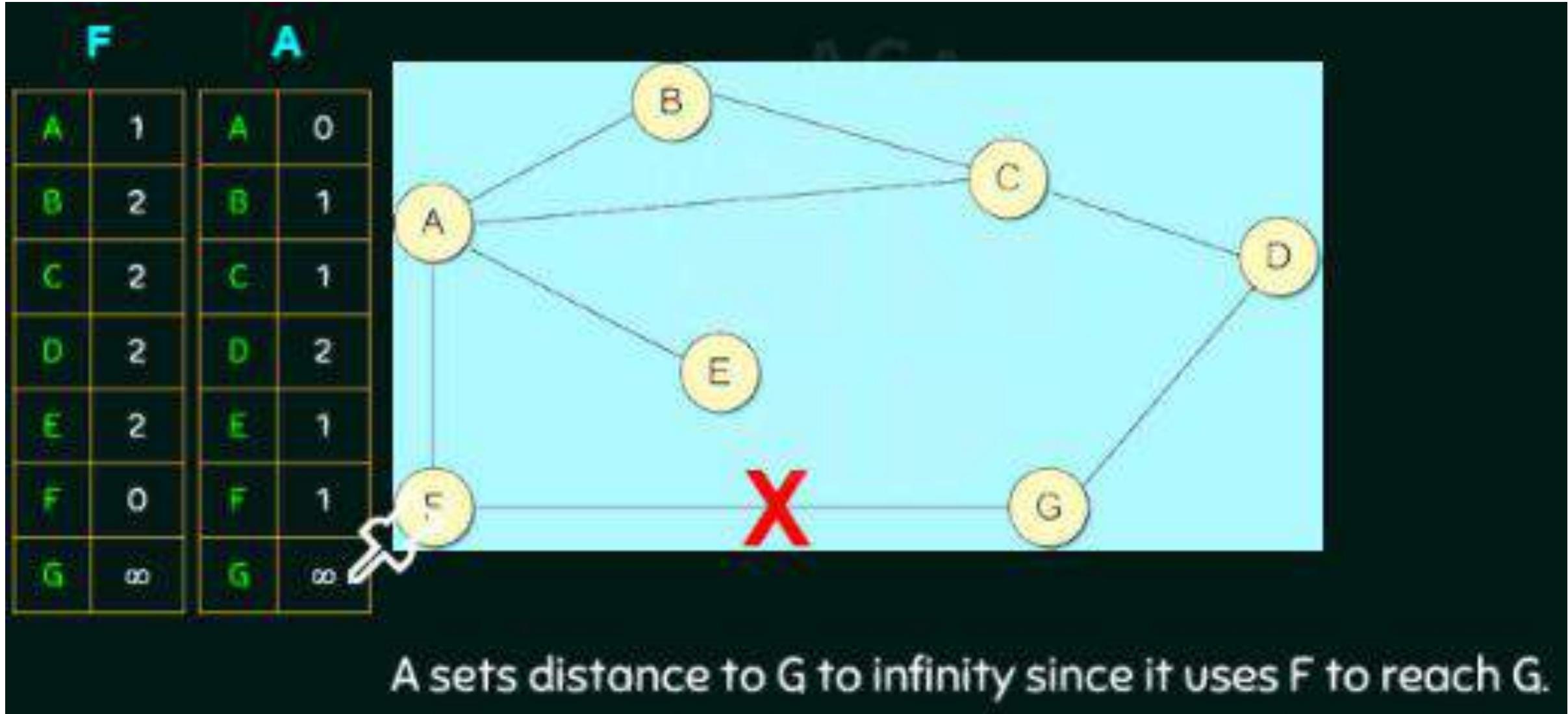
When a Node Detects Link Failure



F detects that link to G has failed.

F sets distance to G to infinity and sends update to A.

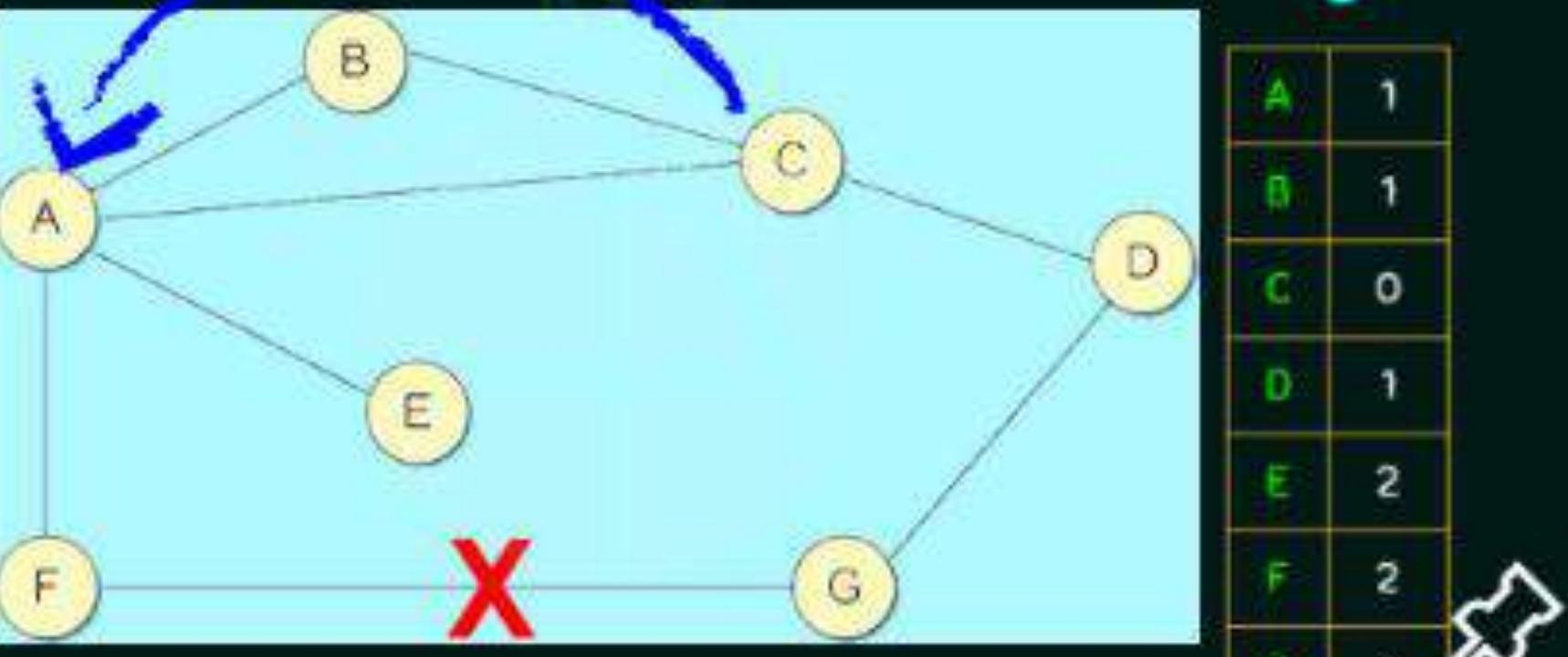
When a Node Detects Link Failure



F A

	A	B	C	D	E	F	G
A	1	A	0				
B	2	B	1				
C	2	C	1				
D	2	D	2				
E	2	E	1				
F	0	F	1				
G	∞	G	∞				

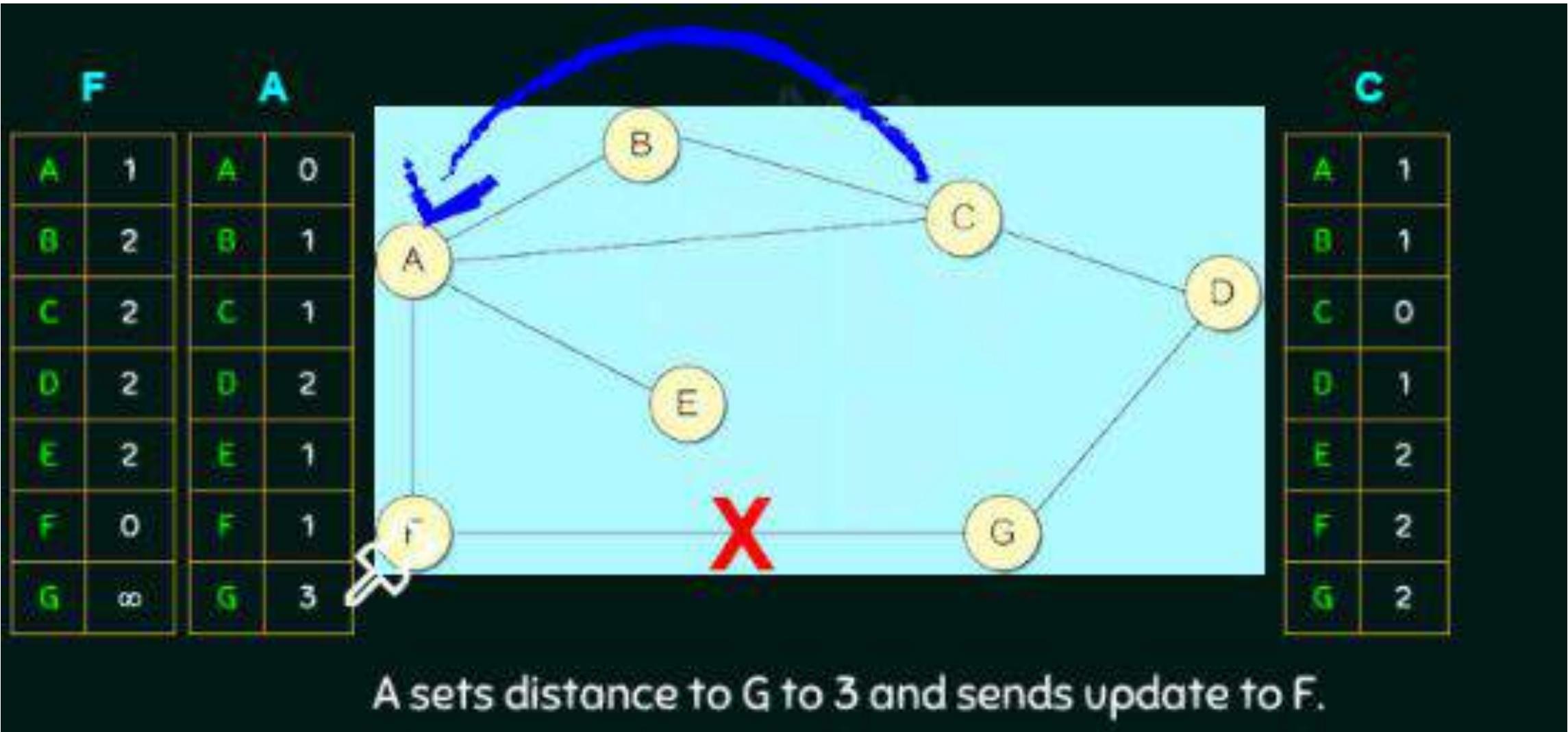
A



C

	A	B	C	D	E	F	G
A	1						
B	1						
C	0						
D	1						
E	2						
F	2						
G	2						

A receives periodic update from C with 2-hop path to G.

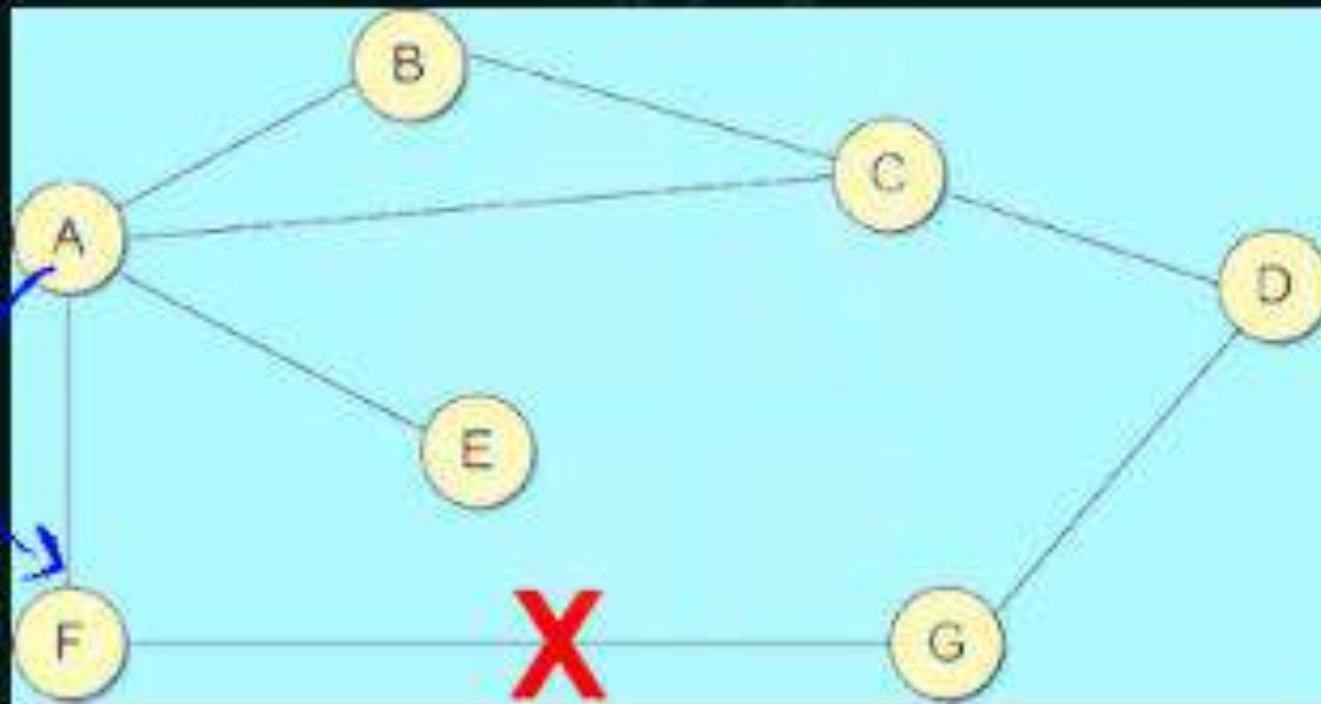


F A

	A	B	C	D	E	F	G
A	1	A	0				
B	2	B	1				
C	2	C	1				
D	2	D	2				
E	2	E	1				
F	0						
G		G	1				3

C

	A	B	C	D	E	F	G
A	1						
B	1						
C	0						
D	1						
E	2						
F	2						
G	2						



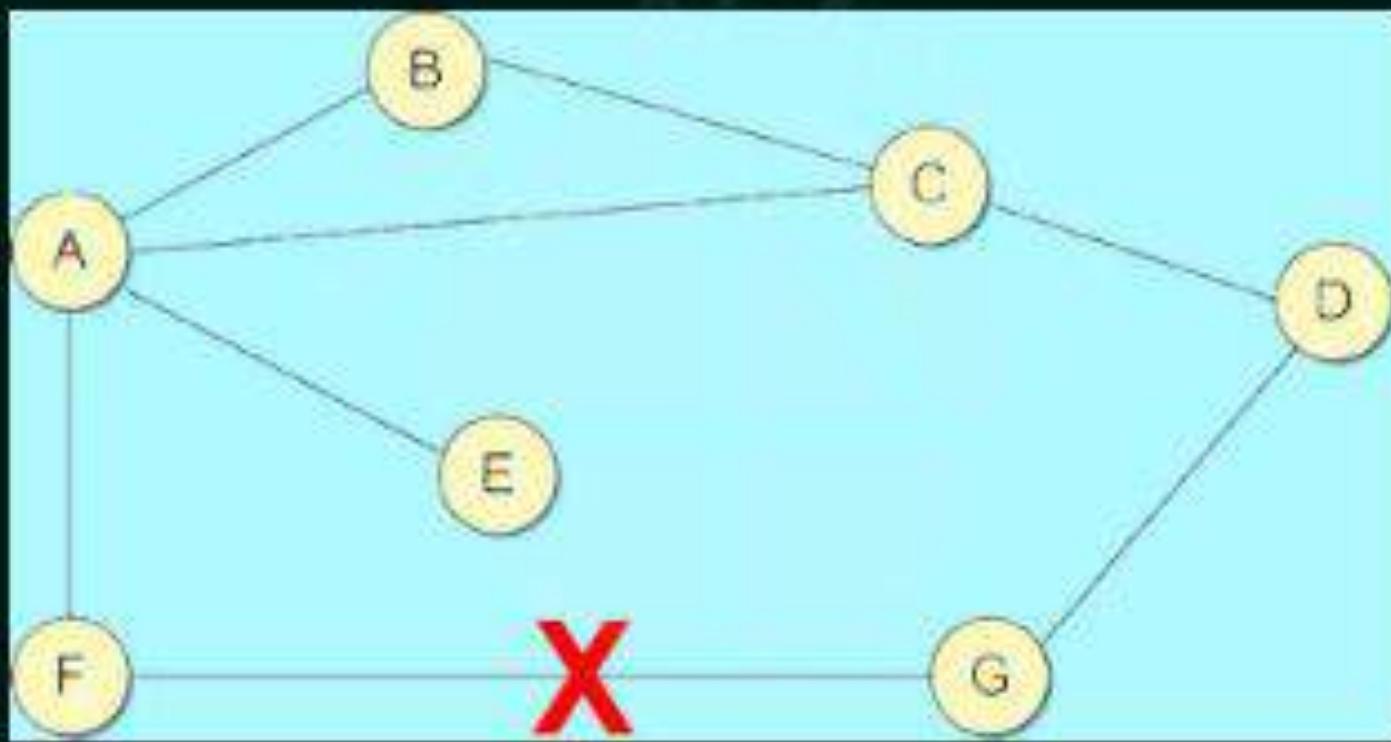
F decides it can reach G in 4 hops via A.

F**A**

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

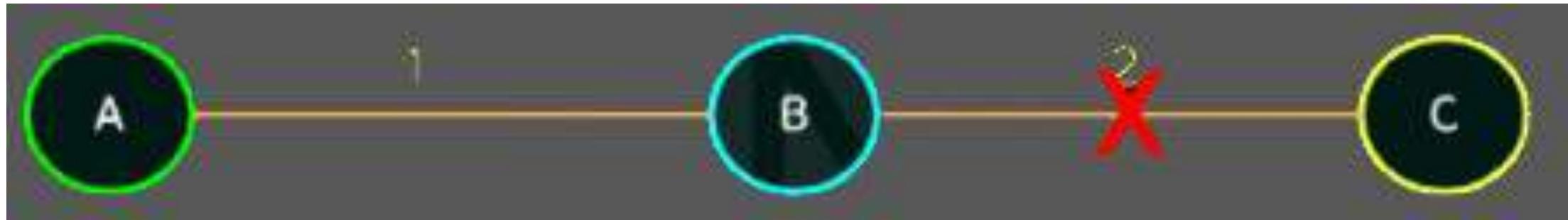
C

	A	B	C	D	E	F	G
A	1						
B	1						
C	0						
D	1						
E	2						
F	2						
G	2						



F decides it can reach G in 4 hops via A.

Count to Infinity problem



A's Routing Table

Dest	Cost	Next Hop
B	1	B
C	3	B

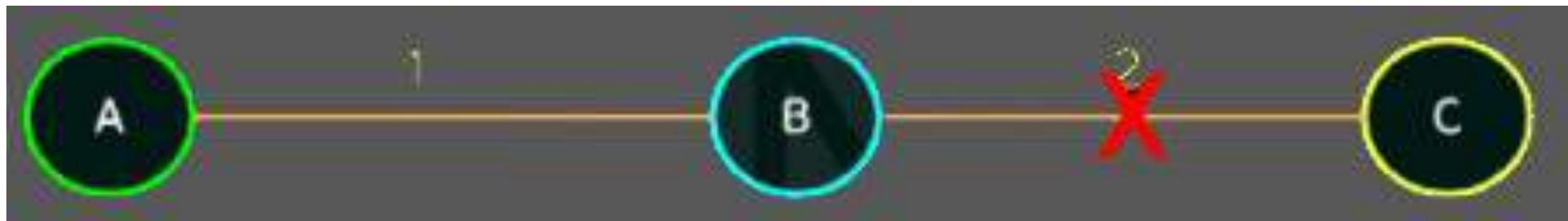
B's Routing Table

Dest	Cost	Next Hop
A	1	A
C	2	C

C's Routing Table

Dest	Cost	Next Hop
A	3	B
B	2	B

Count to Infinity problem



A's Routing Table

Dest	Cost	Next Hop
B	1	B
C	3	B

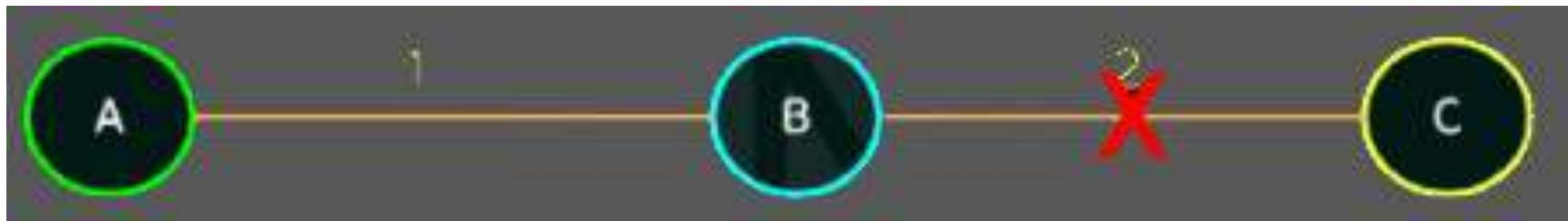
B's Routing Table

Dest	Cost	Next Hop
A	1	A
C	2	C

C's Routing Table

Dest	Cost	Next Hop
A		
B		

Count to Infinity problem



A's Routing Table

Dest	Cost	Next Hop
B	1	B
C	3	B

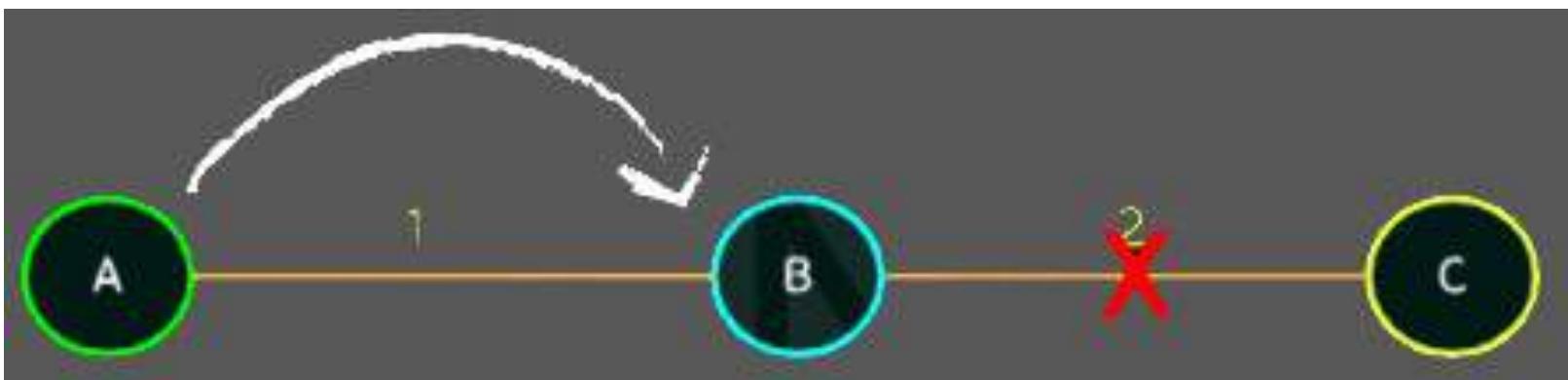
B's Routing Table

Dest	Cost	Next Hop
A	1	A
C		

C's Routing Table

Dest	Cost	Next Hop
A		
B		

Count to Infinity problem



A's Routing Table

Dest	Cost	Next Hop
B	1	B
C	3	B

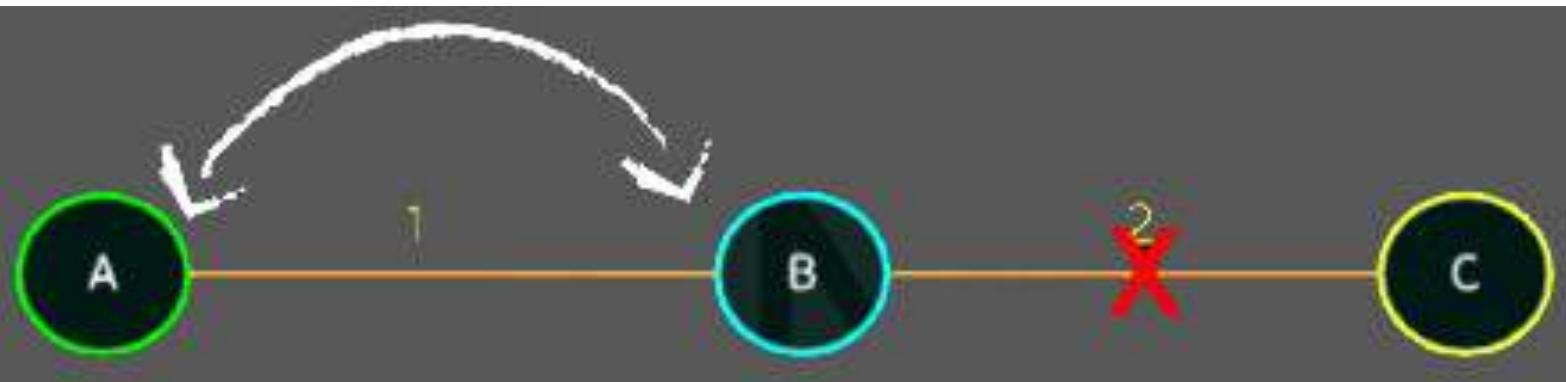
B's Routing Table

Dest	Cost	Next Hop
A	1	A
C	4	A

C's Routing Table

Dest	Cost	Next Hop
A		
B		

Count to Infinity problem



A's Routing Table

Dest	Cost	Next Hop
B	1	B
C	15	B

B's Routing Table

Dest	Cost	Next Hop
A	1	A
C	14	A

C's Routing Table

Dest	Cost	Next Hop
A		
B		

Solution for Count to infinity

- **Split Horizon**
- **Split horizon with Poison Reverse**

Split Horizon

- *In computer network, split-horizon route advertisement is a method of preventing routing loops in distance-vector routing protocols by prohibiting a router from advertising a route back onto the interface from which it was learned.*
- *In other words, it is a method of preventing a routing loop in a network.*
- *The basic principle is simple, information about the routing for a particular packet is never sent back to the direction from which it was received.*

Solution for Count to infinity

Split Horizon

- *With the split-horizon rule in place , this particular loop scenario can not happen, improving convergence time in complex, highly redundant environments.*

Poison Reverse

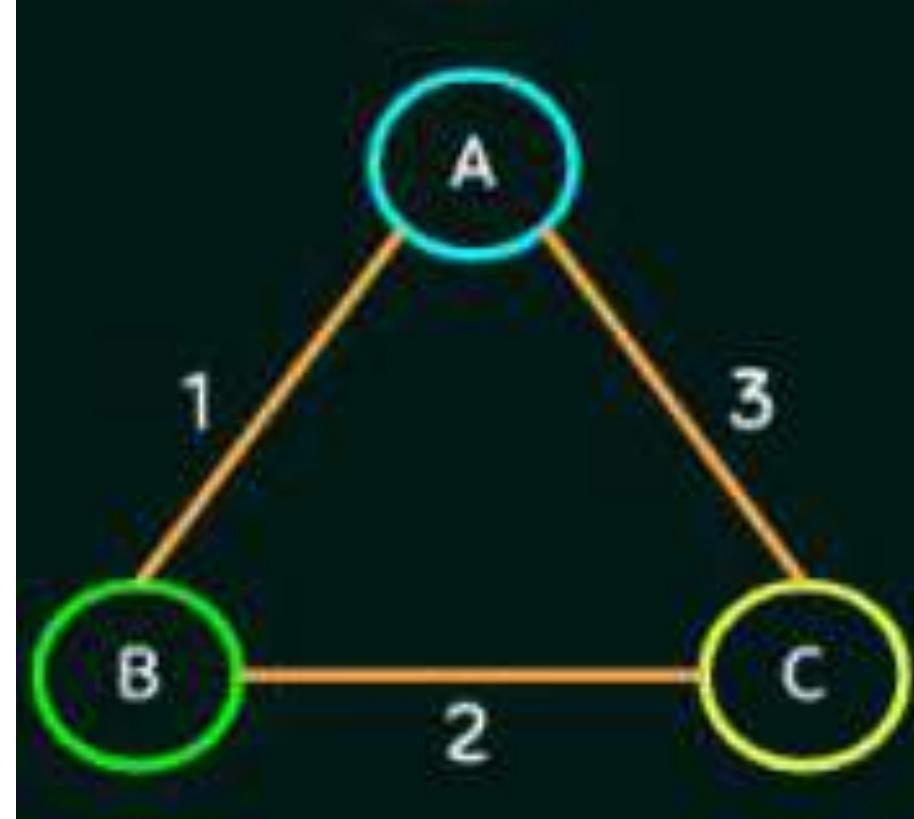
- *Poisson reverse is an implemented algorithm that is often used within distance vector routing.*
- *The use of poison reverse is to solve the count-to-infinity problem. Practically, poison reverse can be thought of as the reverse of split horizon.*
- *With poison reverse, route advertisements that would be suppressed by split horizon are instead advertised with a distance of infinity.*

Poison Reverse

- As A route via B to C and because of that have the cost 3. The poison reverse kicks in when we broadcast our distance vector to our neighbours. The distance table we broadcast is :

To B : [0,1, ∞]

To C: [0,1,3]



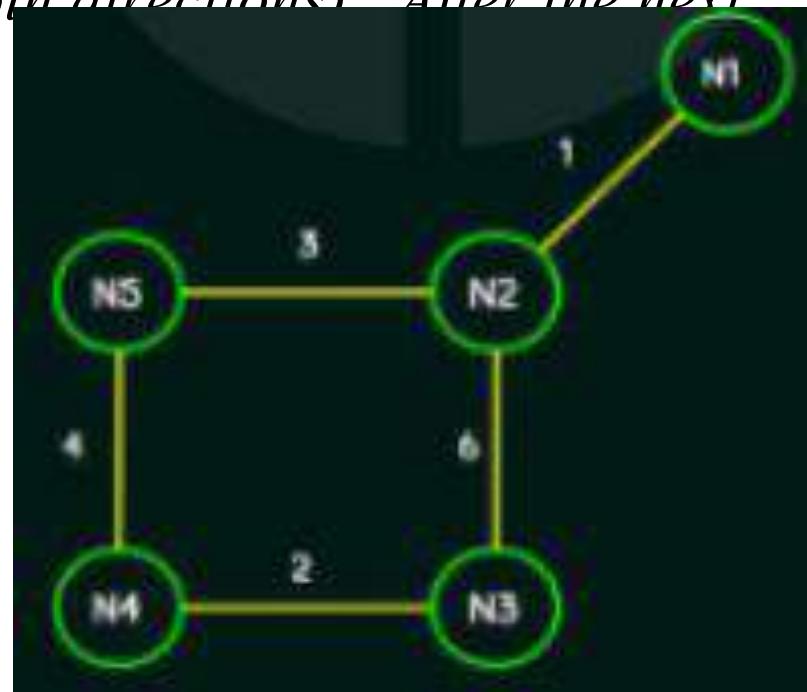
- As we see in the distance vector that is broadcast to node B the end destination C has an infinity value. This solves the count-to-infinity problem since if the link between B and A will not bounce between each other and instead directly try another path.

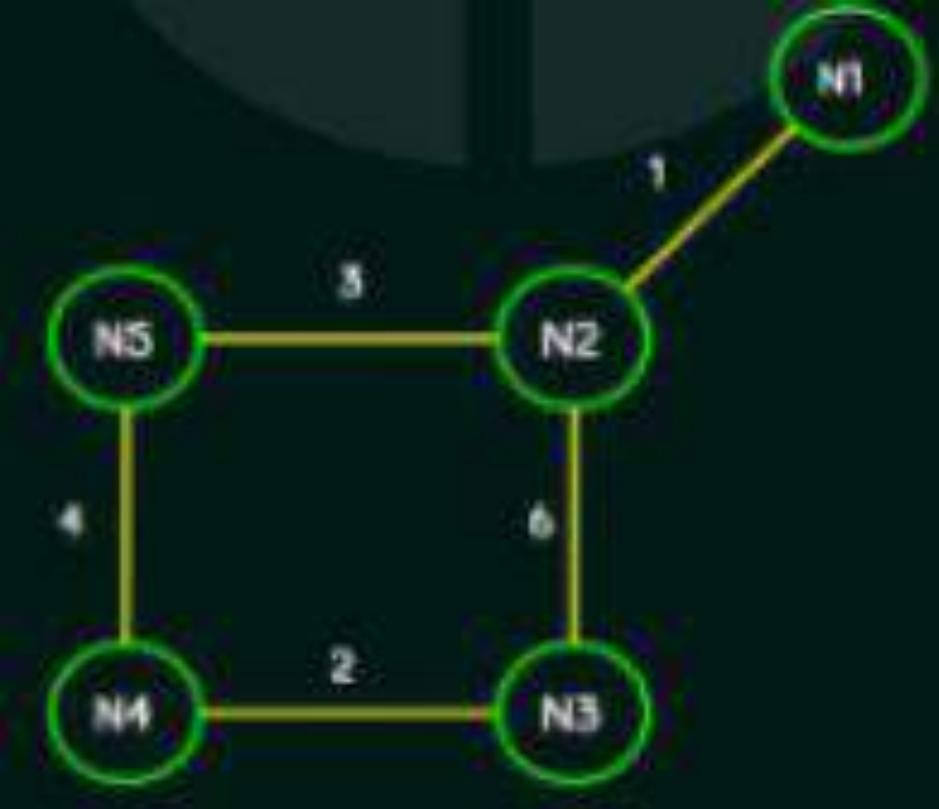
Distance	A	B	C
A	0	1	3
B	1	0	2
C	3	2	0

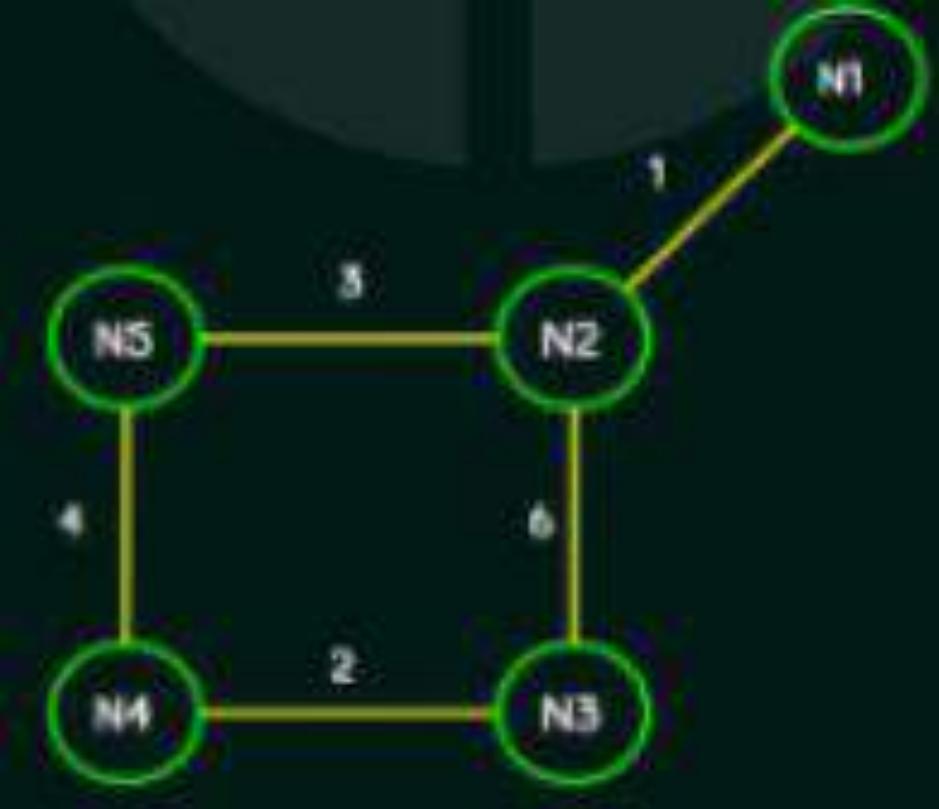
Questions:

Consider a network with five nodes N1 to N5, as shown below. The network uses a Distance Vector Routing protocol. Once the routes have stabilized, the distance vector at different nodes are as following: N1: (0,1,7,8,4) N2: (1,0,6,7,3) N3:(7,6,0,2,6) N4:(8,7,2,0,4) N5:(4,3,6,4,0)

Each distance vector is the distance of the best known path at that instance to nodes N1 to N5, where the distance to itself is 0. Also, all links are symmetric and the cost is identical in both directions. In each round, all node exchanges their distance vectors. In between two rounds, any change in cost of all links will cause the two incident nodes to change only that entry in their distance vectors. The cost of links N2-N3 reduces to 2 (in both directions). After the next round of update what will be the new distance vector at node N3?







RIP Messages

RIP defines two type of messages

- **Request Message:** *Asking a neighbouring RIPv1 enabled router to sends its routing table.*
- **Response Message:** *Carries the routing table of a router.*

RIP Version:

- **RIPv1**
- **RIPv2**
- **RIPng**

RIPv1

RIPv2

RIPng

RIPv1	RIPv2	RIPng
<ul style="list-style-type: none">□ When starting up, and every 30secs thereafter, a router with RIPv1 implementation broadcast to 255.255.255.255 a request message through every RIPv1 enabled interface. □ RIPv1 enabled router not only request the routing tables of other routers every 30 secs, they also listen to incoming requests from the neighbouring routers and send their own routing table in turns.	<ul style="list-style-type: none">□ It includes the ability to carry subnet information thus supporting classless Inter-Domain Routing (CIDR). □ In an effort to avoid unnecessary load on hosts that do not participate in routing, RIPv2 multicast the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast.	<ul style="list-style-type: none">□ ng= Next Generation □ It is an extension of RIPv2 for support of IPV6, the next generation internet protocol. □ The main difference between RIPv2 and RIPng is:<ul style="list-style-type: none">▪ Support of IPV6 networking.▪ While RIPv2 supports authentication, RIPng does not. IPV6 routers were at time, supposed to use IPsec for authentication

RIPv1	RIPv2	RIPng
<ul style="list-style-type: none">□ RIPv1 uses classful routing.□ The periodic routing updates do not carry subnet information, lacking support for variable length subnet mask (VLSM).□ This limitation makes it impossible to have different-sized subnets inside of the same network class. There is also no support for routers authentication, making RIP vulnerable to various attacks.	<ul style="list-style-type: none">□ Unicast addressing is still allowed for special application.□ In RIPv2, MD5 authentication was introduced.□ Route tags were also added in RIPv2. This functionality allows a distinction between routes learned from the RIP protocol and routes learned from other protocols.	<ul style="list-style-type: none">□ RIPv3 encodes the next-hop into each route entry, RIPng requires specific encoding of the next hop for a set of route entries.□ RIPng sends updates an UDP port 521 using the multicast group FF02::9

Link state Routing

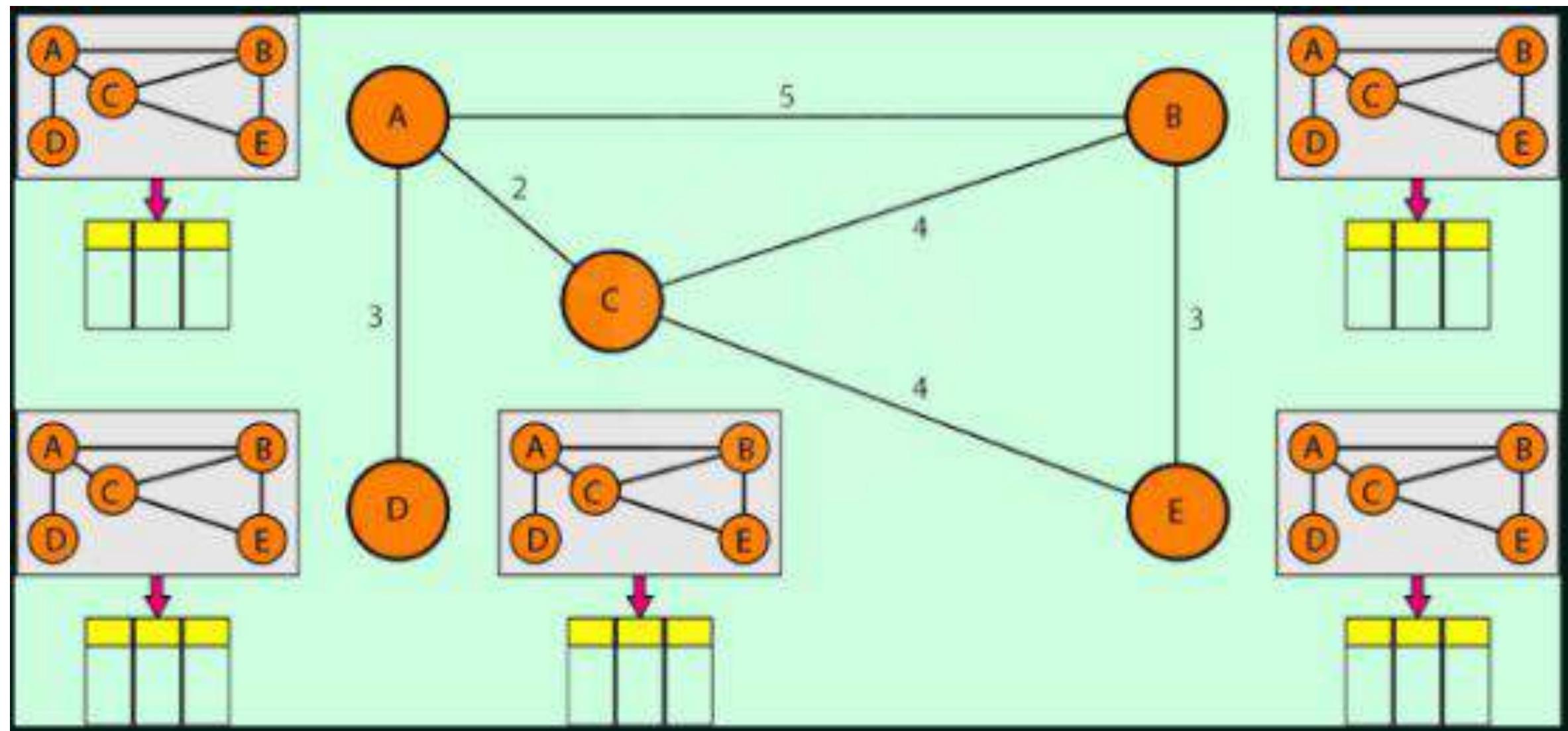
- **Link+State**
- Link state routing (LSR) has a different philosophy from the DVR (Distance Vector Routing). In LSR, each node has the entire topology of the network.

Link State	Distance Vector
<input type="checkbox"/> Complete topology.	<input type="checkbox"/> Local topology
<input type="checkbox"/> Flooding	<input type="checkbox"/> Exchange
<input type="checkbox"/> Global	<input type="checkbox"/> Decentralized
<input type="checkbox"/> “Tell the world about neighbours”	<input type="checkbox"/> “Tell the neighbours about the world”

Link state Routing

- A Link state *packet* can carry a large amount of information.
- Link state packet contains:
 - *ID of the node that created the LSP.*
 - *Cost of the link to each directly connected neighbour*
 - *Sequence number (SEQNO)*
 - *Time-to-Live (TTL) for this packet.*

Link state Routing



Link state Routing

- **Strategy:** *Send all nodes (not just neighbours) information about directly connected links (not entire routing table).*
- **Idea:** *LSR in two phases:*
 - *Phase 1: Reliable flooding*
 - *Initial state: each node knows the cost of its neighbours*
 - *Final state: Each node knows the entire network topology*
 - *Phase 2: Route calculation*
 - *Each node uses Dijkstra's algorithm on the graph to calculate optimal routes to all nodes.*

Link state Routing

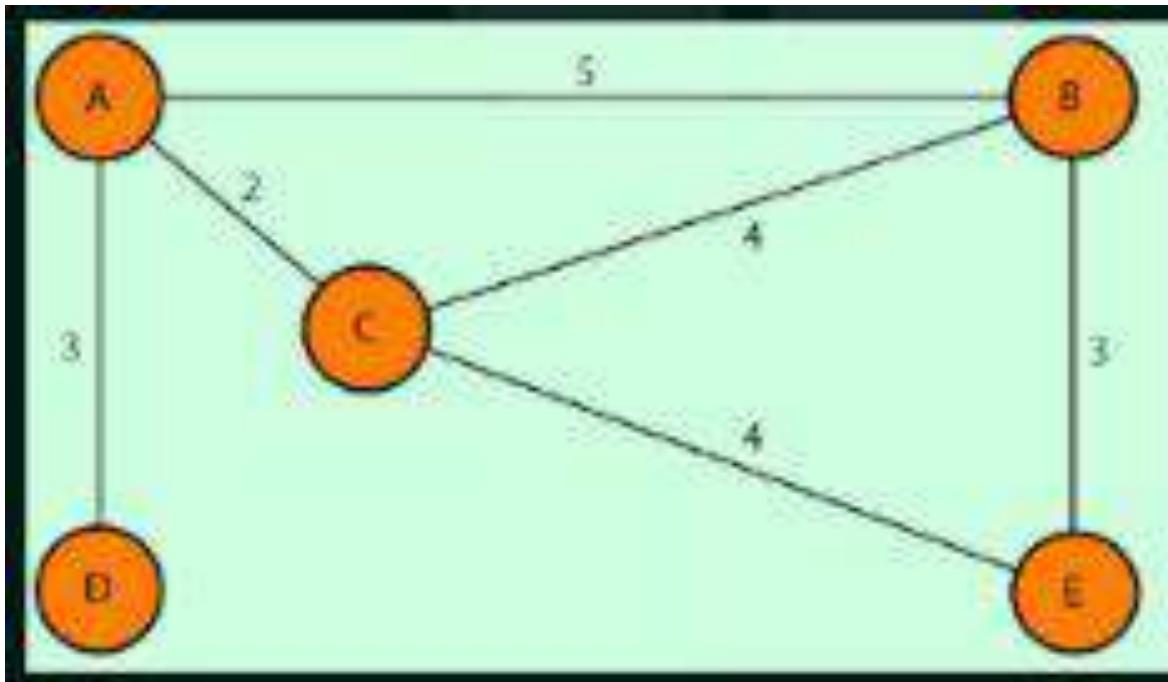
- The Link state packet contains:
 - *ID of the node that created the LSP.*
 - *Cost of the link to each directly connected neighbour*
 - *Sequence number (SEQNO)*
 - *Time-to-Live (TTL) for this packet.*

- LSP are generated in two occasions:
 - *Triggered*
 - *Periodic*

Link state Routing

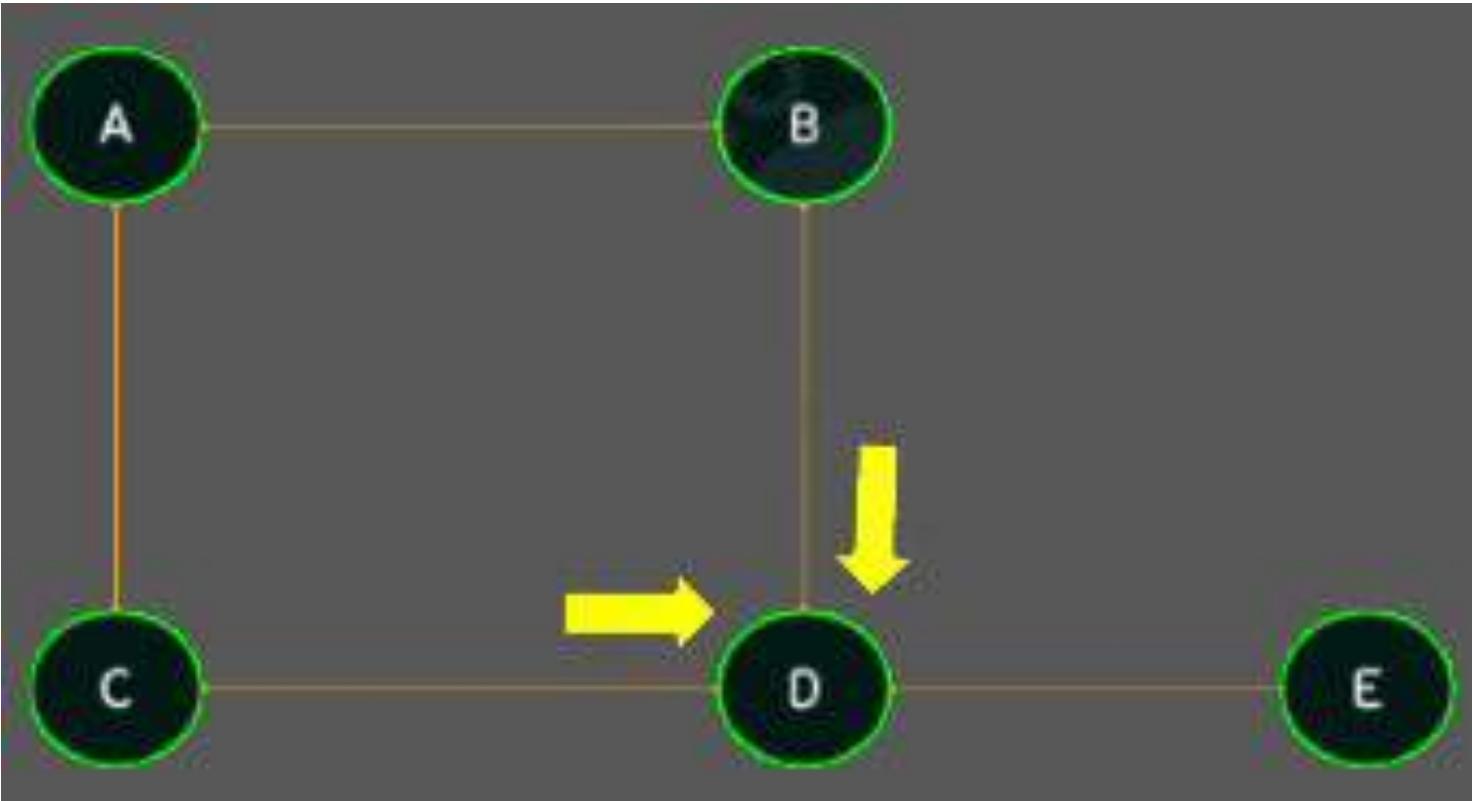
□ Phase 1: Reliable flooding

- *Store most recent LSP from each node.*
- *Forward LSP to all nodes but one that sent it.*
- *Generate new LSP periodically, increment SEQNO.*
- *Start SEQNO at 0 when reboot.*
- *Decrement TTL of each stored LSP, discard when TTL = 0.*



Reliable Flooding in Link state Routing

- *The node D will receive same LSP packet from both B and C but will discard the packet with old SEQNO number and retain the packet with new SEQNO.*



Features and Solution of LSP

Feature	Responsible field of the LSP
□ Minimise the number of messages and detect duplicated	□ ID field in the LSP.
□ Newer information should precede older info	□ Sequence number field in the LSP
□ Exhaust of sequence number	□ 32 bits sequence number field in LSP
□ Looping of LSPs.	□ TTL field in LSP.

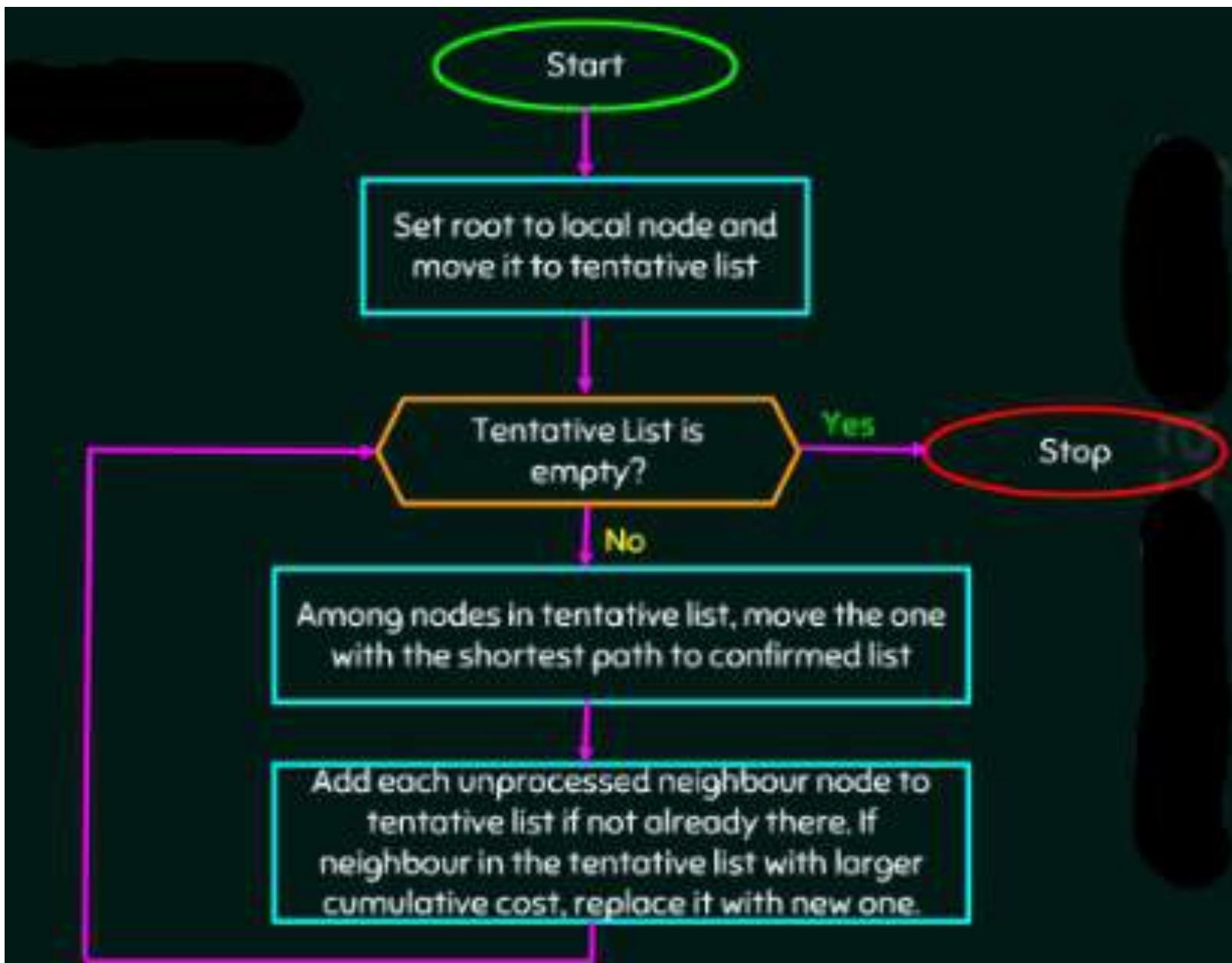
LSP vs DVR

Feature	Link State Routing	Distance Vector routing
□ Topology	□ Complete topology	□ Local topology
□ Communication type	□ Flooding	□ Exchange
□ Convergence	□ Fast	□ Slow
□ Routing Loops	□ Less Prone	□ Highly Prone
□ Algorithm	□ Dijkstra's Algorithm	□ Bellman Ford Algorithm
□ Metrics	□ Cost	□ Hop count
□ Updates	□ Triggered, Partial	□ Frequent, Periodic
□ Scalability	□ Highly scalable	□ Limited
□ Protocols	□ OSPF, IS-IS	□ RIP, IGRP

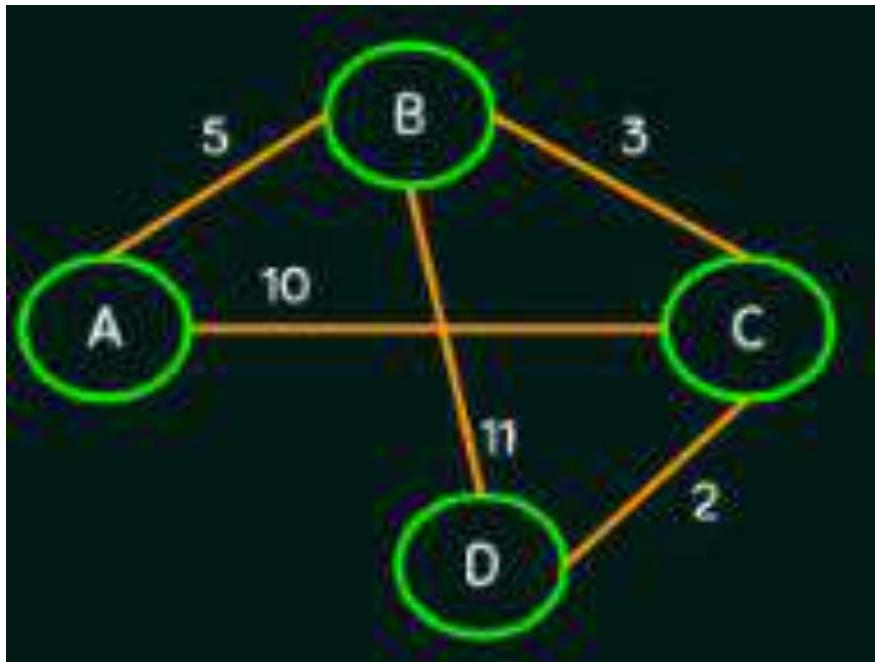
Shortest Path Routing

- *In practice each router computes its routing table directly from LSP's it has collected using a realization of Dijkstra's algorithm.*
- *Specially each router maintains two lists:*
 1. *Tentative list*
 2. *Confirmed List*
- *Each of these lists contains a set of entries of the form (Destination, Cost, Next hop)*
E.g. (A, 5, C)

Dijkstra's Algorithm



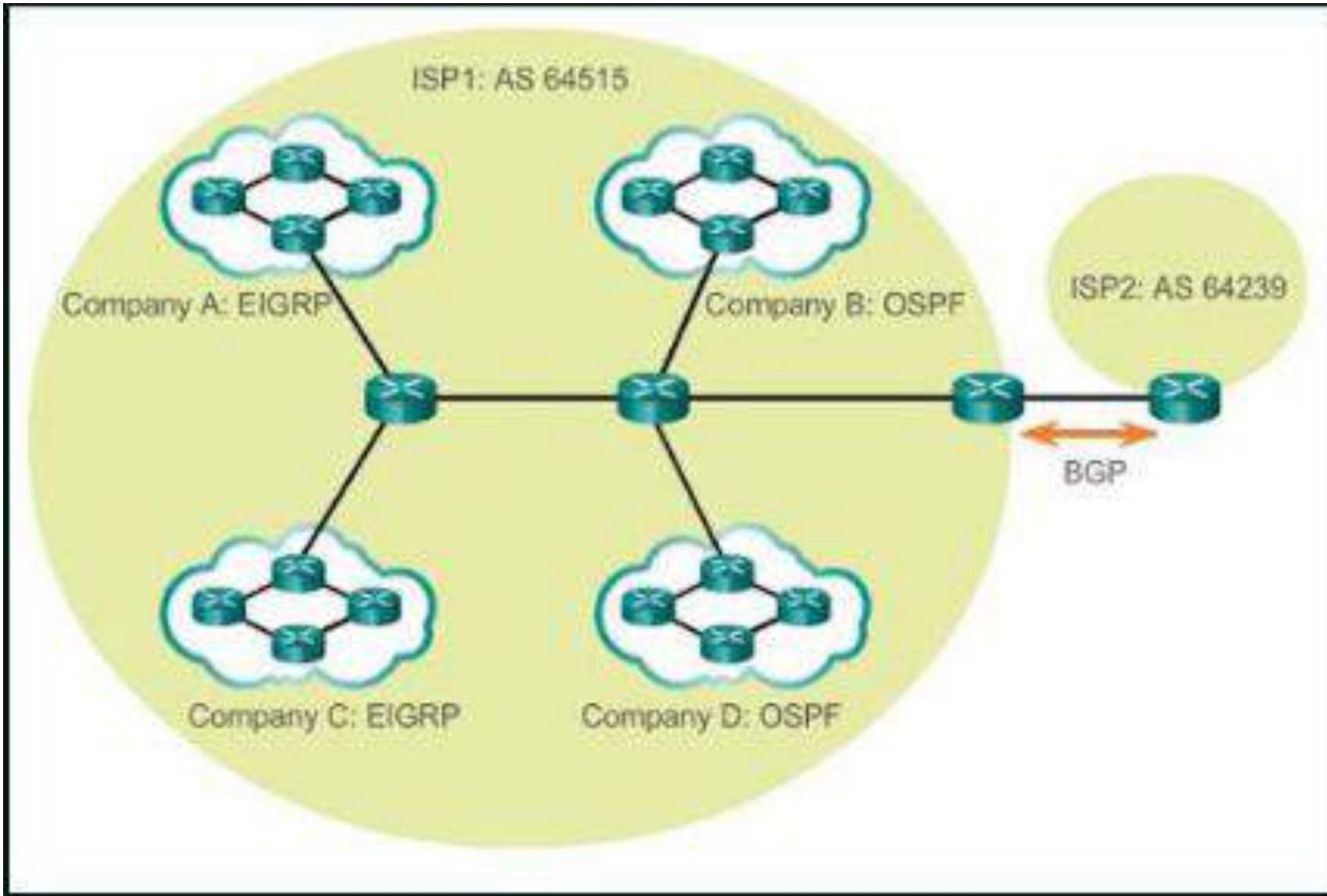
Question: Find the shortest path routing for the following graph.



Open Shortest Path First (OSPF)

- *OSPF is a routing protocol for IP networks with used link state routing algorithm.*
- *OSPF falls into the group of IGPs (Interior Gateway protocols, operating within a single Autonomous system (AS).*
- *RIP uses hop count as a metric whereas OSPF uses cost as the metric.*
- *OSPF was developed so that the shortest path through a network was calculated based on the cost of the route.*
- *The link cost is calculated by taking bandwidth, delay and load into account.*

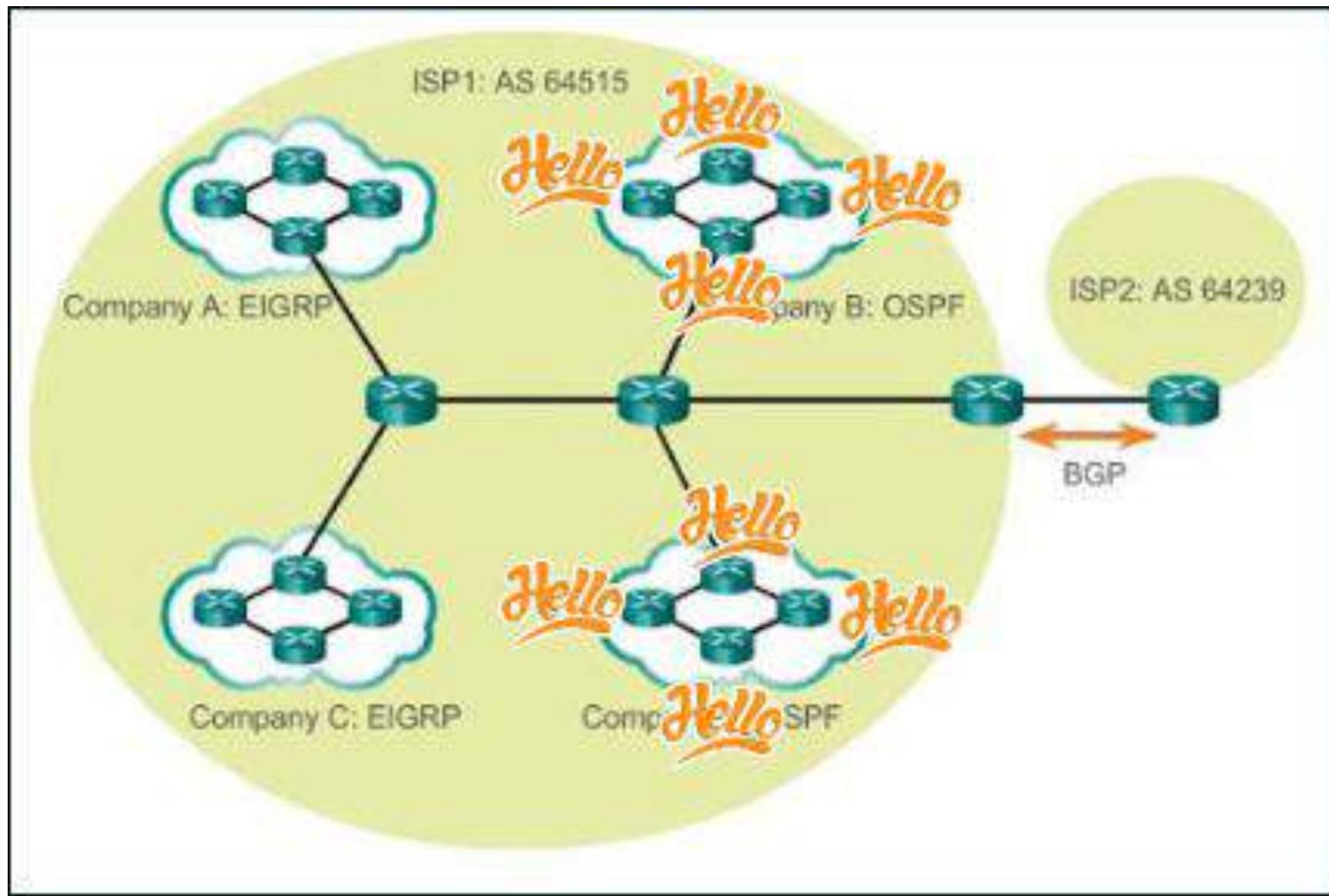
Autonomous System



Open Shortest Path First (OSPF)

- *OSPF undertakes route cost calculation on the basis of link-cost parameters, which can be weighted by the administrator.*
- *OSPF is reliable even for large and complex networks.*
- *As a link state routing OSPF maintains link-state databases. The state of a given route in the network is the cost, and OSPF algorithm allows every router to calculate the cost of the routes to any given reachable destination.*
- *An router interface with OSPF will then advertise its link cost to neighbouring routers through multicast, known as the HELLO procedure.*
- *The link cost is calculated by taking bandwidth, delay and load into account. All routers with OSPF implementation keep sending HELLO packets, and thus changes in the cost of their links become known to neighbouringouters.*

OSPF HELLO procedure

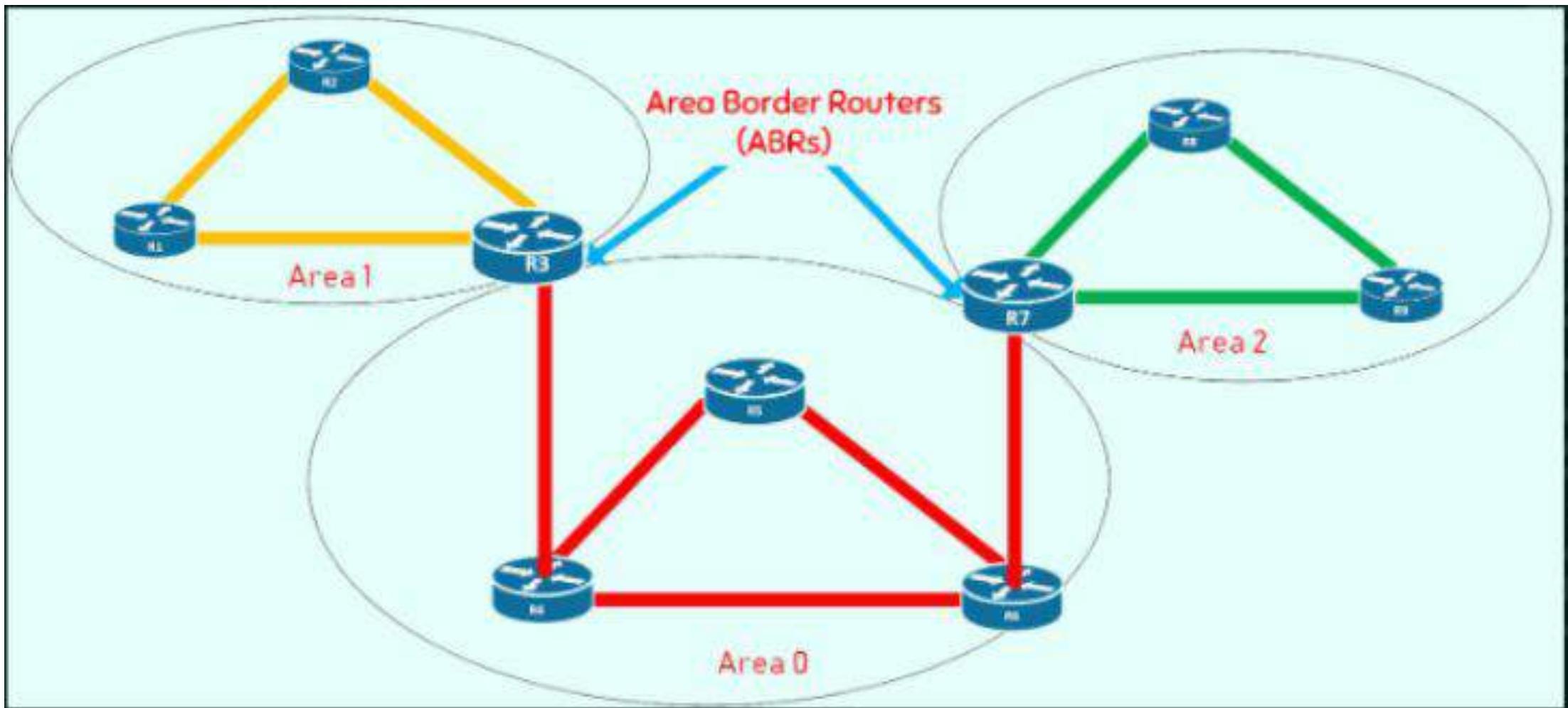


Open Shortest Path First (OSPF)

- *An OSPF network can be structured, or subdivided, into routing areas to simplify administration and optimize traffic and resource utilization.*
- *Area are identified by 32-bits numbers, expressed either simply in decimal, or often in the same dot-decimal notation used for IPV4 addresses.*
- *By convention, area 0 (zero), or 0.0.0.0 represents the core or backbone area of an OSPF network.*
- *While the identification of other areas may be chosen at will, administrators often select the IP address of a main router in an area as the area identifier.*
- *Each additional area must have a connection to the OSPF backbone area. Such a connections are maintained by an interconnecting router, known as an Area Border Router (ABR).*

Open Shortest Path First (OSPF)

- *An ABR maintains separate link-state databases for each area it serves and maintain summarized routes for all areas in the network.*
- *OSPF detects changes in the topology, such as link failures, and converges on a new loop-free routing structure within seconds.*
- *OSPF supports complex networks with multiple routers, including backup routers, to balance traffic load on multiple links to other subnets.*

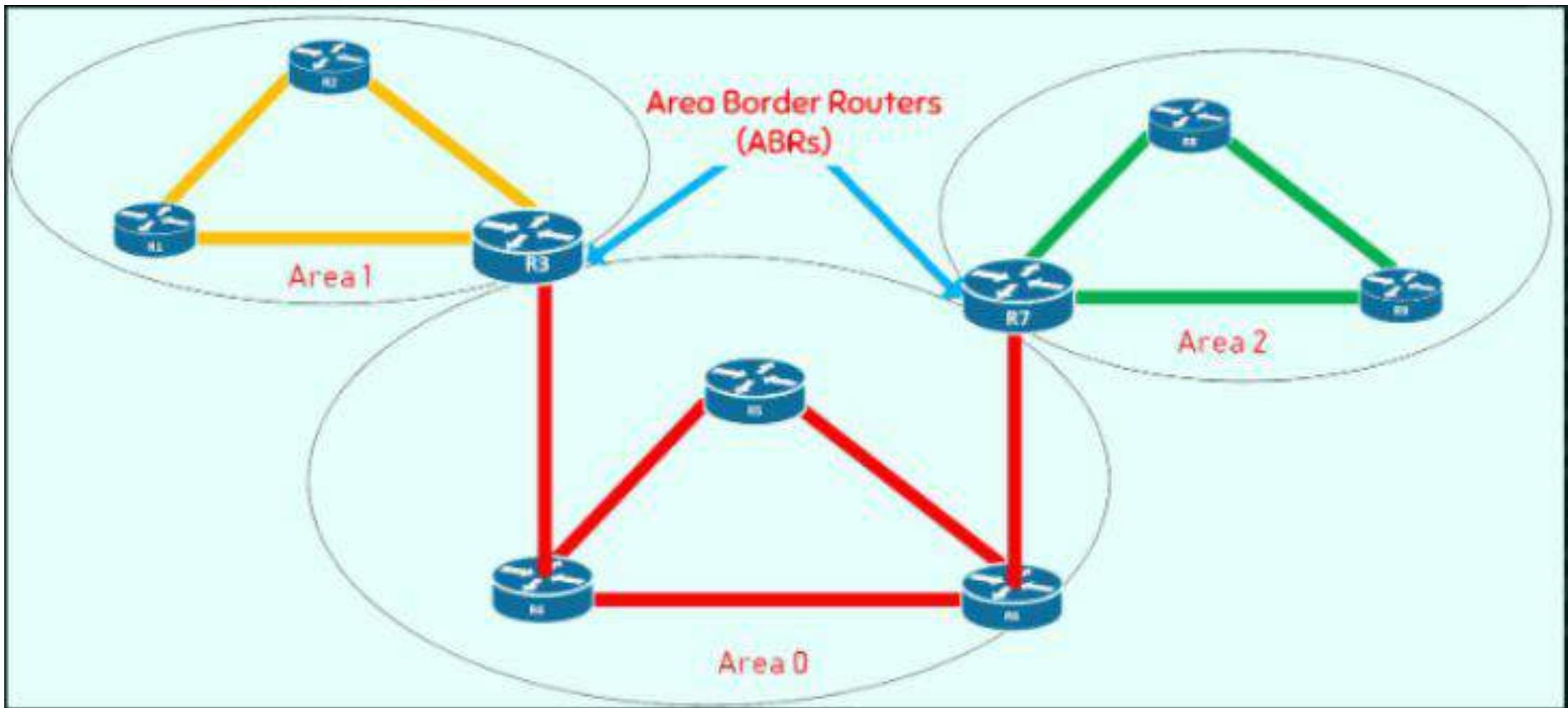


Open Shortest Path First (OSPF)

- *As a link state routing protocol, OSPF establishes and maintains neighbour relationships for exchanging routing updates with other routers.*
- *The neighbour relationship table is called adjacency database.*
- *Two OSPF routers are neighbours if they are members of the same subnet and share the same IP, subnet mask, timers and authentication.*
- *In essence, OSPF neighbourhood is a relationship between two routers that allow them to see and understand each other but nothing more. OSPF neighbours do not exchange any routing information –the only packets they exchange are HELLO packets.*

Open Shortest Path First (OSPF)

- *OSPF adjacencies are formed between selected neighbours and allow them to exchange routing information.*
- *Two routers must first be neighbours and then only then ,can they become adjacent.*
- *Two routers become adjacent if at least one of them is Designated router or Backup Designated Router (on multi-access type networks), or they are interconnected by a point-to-point or point-to-multipoint network type.*
- *For forming a neighbour relationship between, the interfaces used to form the relationship must be in the same OSPF area.*



Open Shortest Path First (OSPF)

- *Each OSPF router within a network communicates with other neighbours routers on each connecting interface to establish the states of all adjacencies.*
- *Every such communication sequence is a separate conversation identified by the pair of router IDs of the communicating neighbours.*
- *During its course, each router conversation transitions through a maximum of eight conditions defined by a state machine*

OSPF States

1. Down
2. Attempt
3. Init
4. 2-way
5. Exstart
6. Exchange
7. Loading
8. Full

Open Messages

- ❑ OSPF defines five different message types, for communication:

Type 1	Hello	Neighbors
Type 2	Database Description (DBD)	Adjacencies
Type 3	Link State Request (LSR)	
Type 4	Link State Update (LSU)	
Type 5	Link State Acknowledgment (LSAck)	Reliable Update

OSPF routers Type

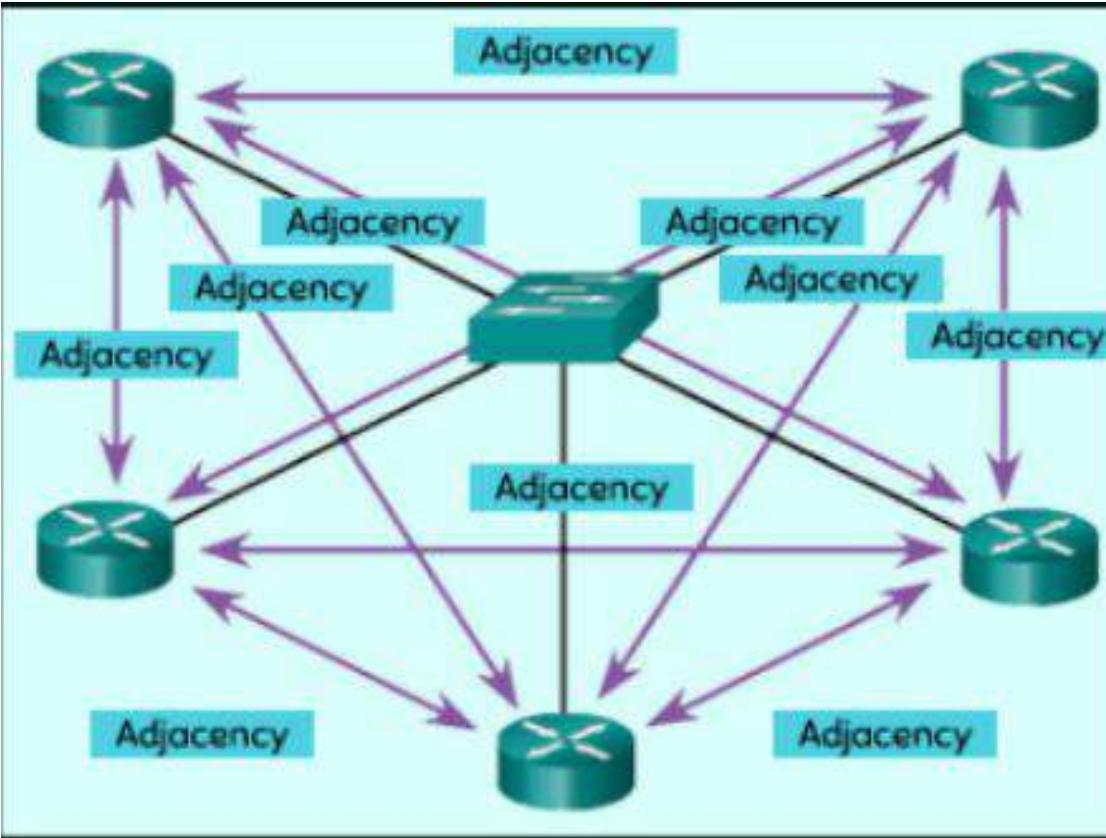
OSPF defines the following overlapping categories of routers:

- **Internal Routers (IR):** *An internal router has all its interfaces belonging to the same area.*
- **Area Border Router (ABR):** *An ABR is a router that connects one or more areas to the main backbone network. It is considered a member of all area it is connected to.*
- **Backbone Router (BR):** *A backbone router has an interface to the backbone area. Backbone routers may also be area routers, but do not have to be.*
- **Autonomous System Boundary Router (ASBR):** *AN ASBR connects one AS with another or the internet.*

OSPF Routers Type

OSPF defines the following overlapping categories of routers:

- Designated Router (DR)
- Backup Designated Router (DBR)



- If number of routers N , then number of adjacencies $\frac{N(N-1)}{2}$
- Example for 3 routers $\frac{3(3-1)}{2} = 3$ number of adjacencies.

Transport layers

Application → In this layer application related data is generated.

Presentation → Here data is being compressed, encrypted

Session → ^{red} Dialog exchange (Dialog control activities)

Transport → It is responsible for process to process delivery of the entire message.

Network

Link

Physical

Suppose at the host multiple processes are running. Suppose transport layer responsibility is to identify uniquely each host process and deliver the generated data to the intended host process. To do this each process is associated with a unique port number.

Network layer or Internet protocol layer identifies networks with these unique IP addresses. Host-to-host data delivery is done by data link layer.

MAC address — Hardware address of the devices

Services provided by Transport layer:-

1. Port addressing (Source and destination port no. are added to the data generated by the application layer and carried by the transport layer)
2. Segmentation and Reassembly
3. Connection control (connection oriented and connectionless).
4. Flow control (speed control)
5. Error control activity

Two important Transport layer protocols are

- ① TCP
- ② UDP

Transport layer

Application → In this layer application related data is generated.

Presentation → Here data is being compressed, encryption, red.

Session → Dialog exchange (dialog control activities)

Transport → It is responsible for process to process delivery of the entire message.

Network Layer

Network Layer

Physical

Suppose at the host multiple processes are running. Suppose transport layer responsibility is to identify uniquely each host process and deliver the generated data to the intended host process. To do this each process is associated with a unique port number.

Network layer or Internet protocol layer identifies networks with these unique IP addresses. Host-to-host data delivery is done by data link layer.

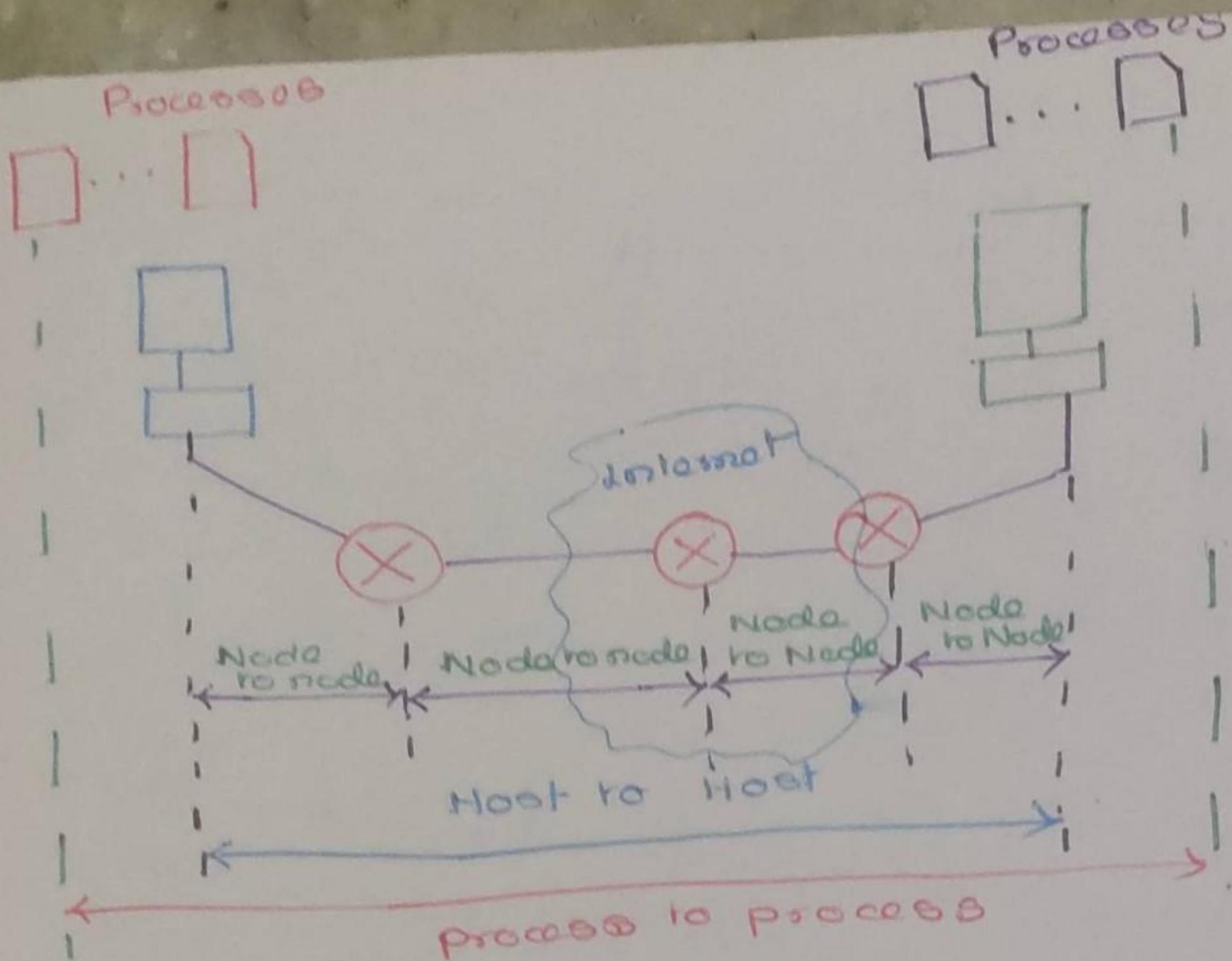
MAC address — Hardware address of the devices

Services provided by Transport layer:-

1. Port addressing (Source and destination port no. are added to the data generated by the application layer and carried by the transport layer)
2. Segmentation and Reassembly
3. Connection control (connection oriented and connectionless).
4. Flow control (speed control)
5. Error control activity

Two important Transport layer protocols are

- ① TCP
- ② UDP



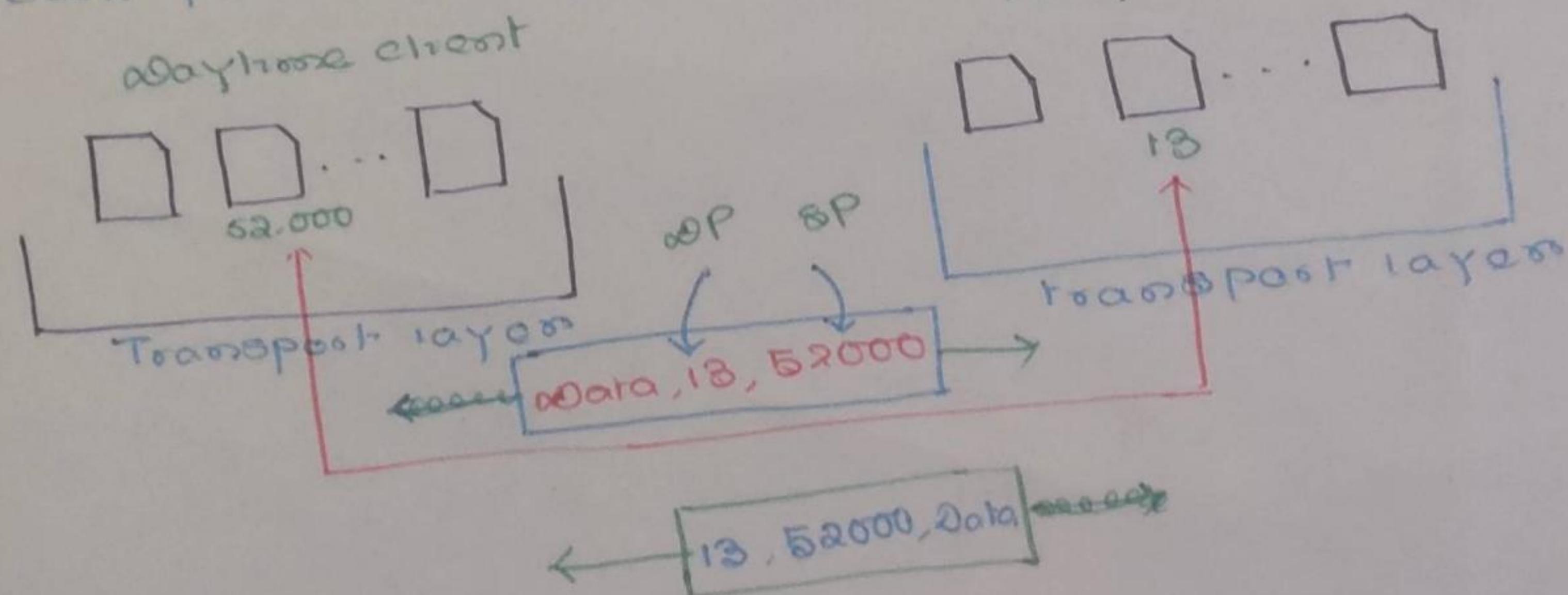
Node to Node: Data link layer (IP address)

Host to Host: Network layer (Port no.)

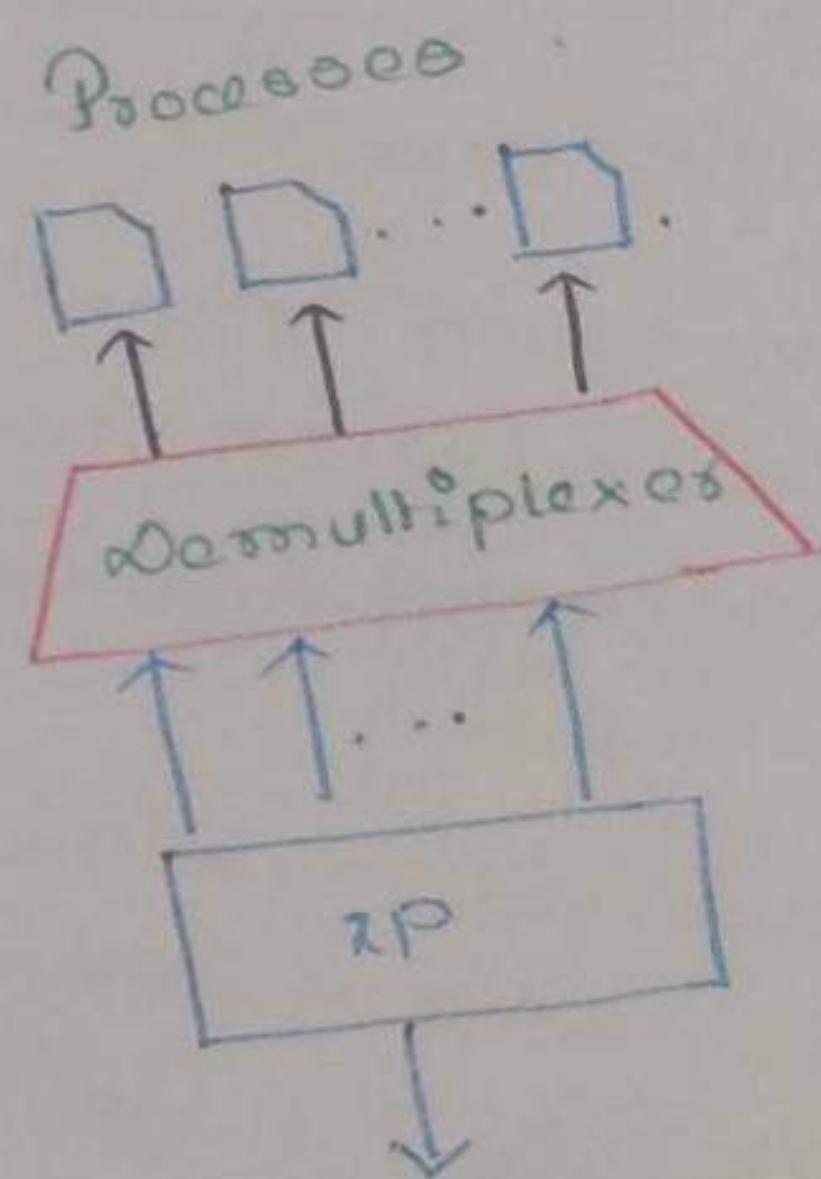
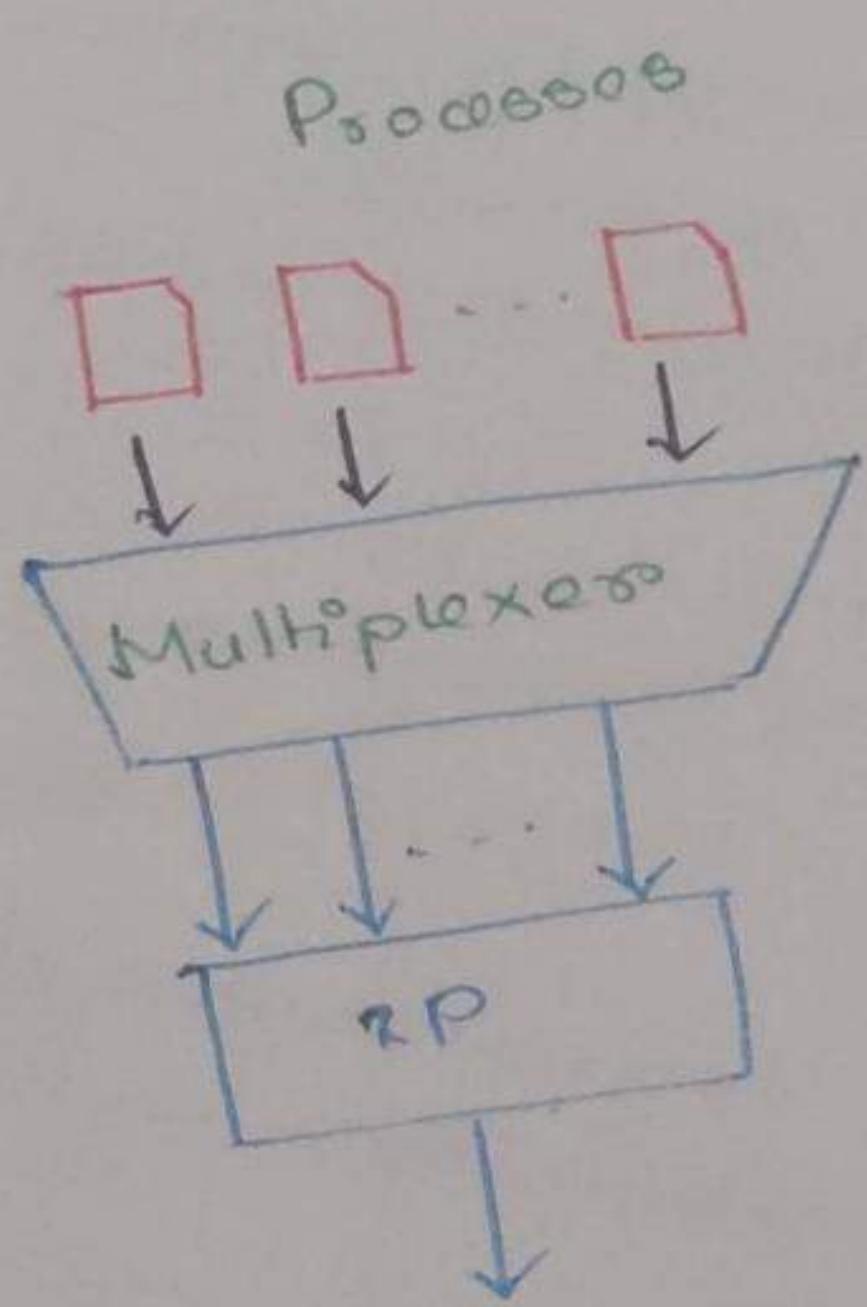
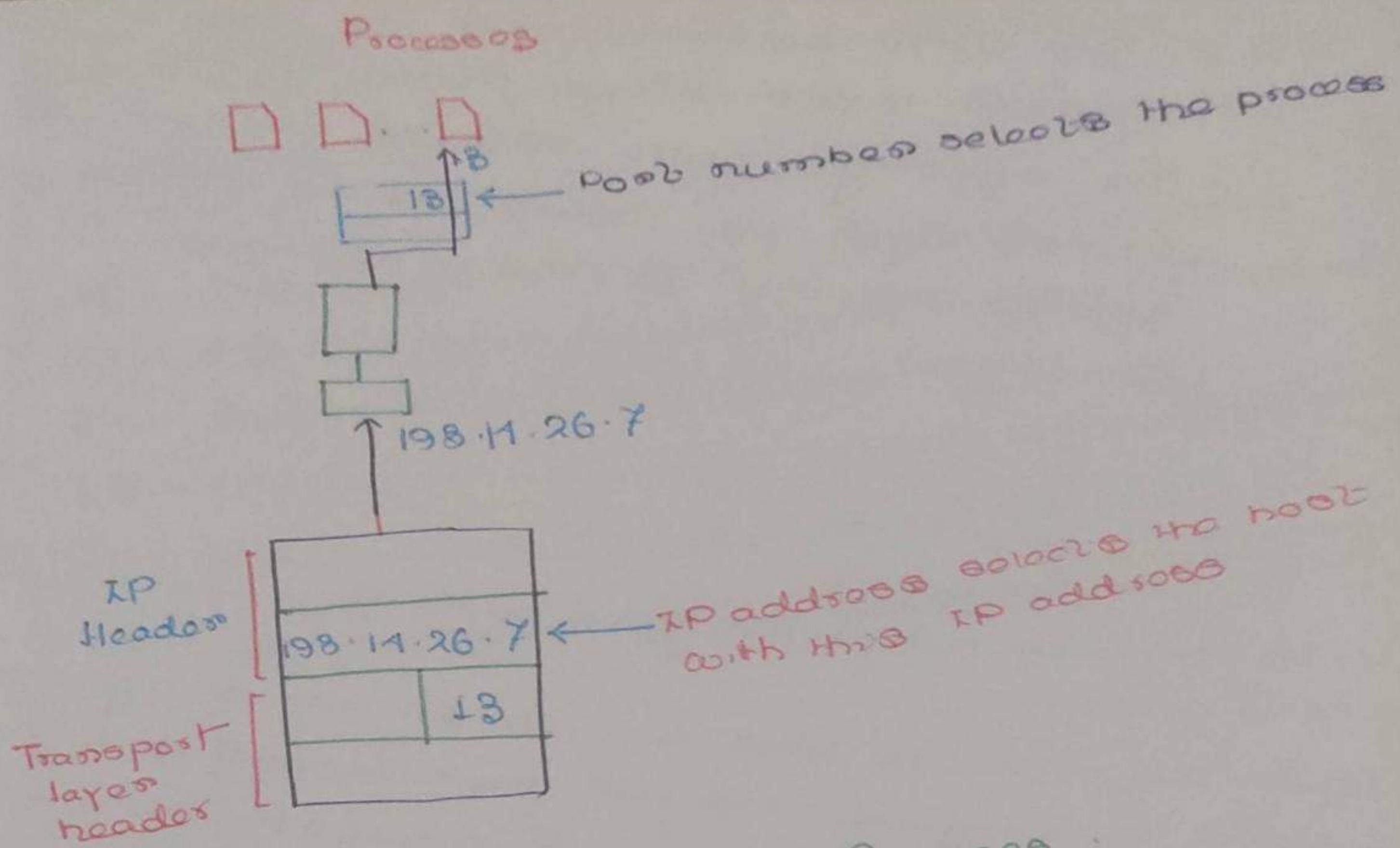
Process to Process: Transport layer (Port no.)

Each process is identified by a unique port no.

Day home servers



DP = Destination Port No.
SP = Source Port No.



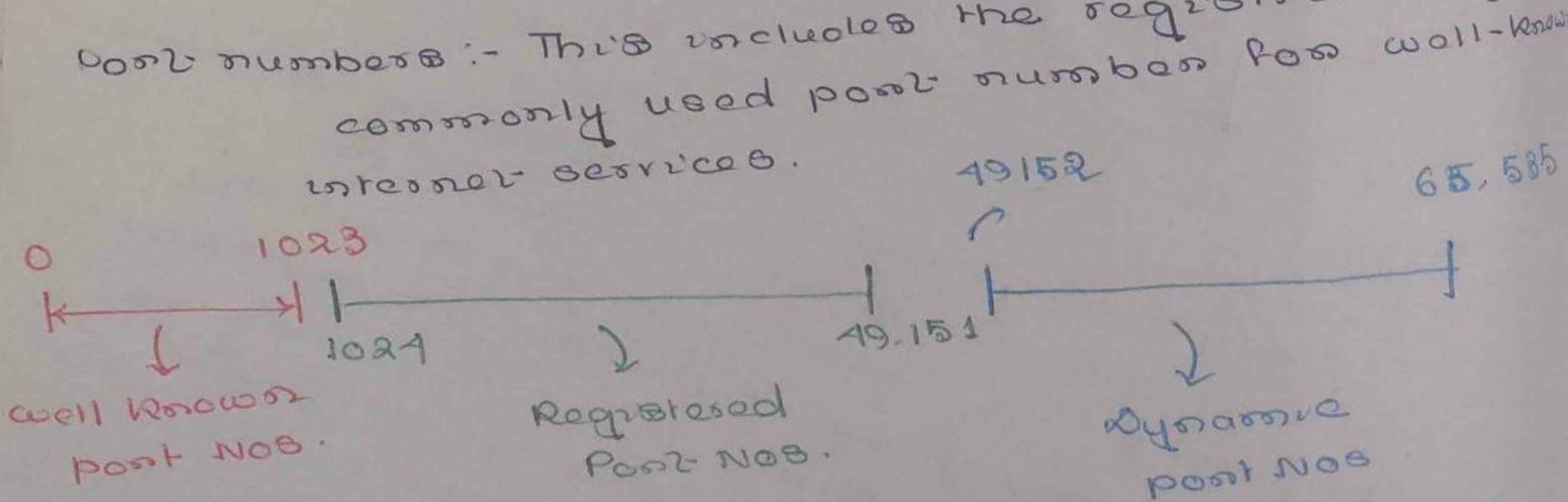
Multiplexing and Demultiplexing vs done at the transport layer. As many processes are running at once in the application layer. But only one transport layer is present. So multiplexing vs done and port addresses are embedded to the next layer that is transferred to the network layer and is at the receiver side after receiving the network layer datagram the network layer headers will be removed and

The packet will be transferred to the transport layer. After demultiplexing the message with specific port address will be delivered to the specific process at the receiver device.

Port Numbers:-

- (1) In computer networking, a port is a communication end point.
- (2) At the software level, within an operating system a port is a logical construct that identifies a specific process or a type of network service.
- (3) A port is identified for each transport protocol and address combination by a 16-bit unsigned number, known as the port number.
- (4) The most common transport protocols that use port numbers are the TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Port numbers :- This includes the registration of commonly used port numbers for well-known interior services.



The port numbers are divided into three ranges

- ① Well Known
- ② Registered
- ③ Dynamic or Private ports.

2. Registered Port Numbers

The registered ports are those from 1024 through 49,151.

- * IANA (Internet Assigned Numbering Authority) maintains the official list of well-known and registered ranges.
- * IANA is responsible for the global coordination of the DNS root, IP addressing, and other internet protocol resources.
- * This includes the registration of commonly used port numbers for well-known internet services.

3. Dynamic Port Numbers :- (Private port numbers)

Range from 49,152 to 65,535 (i.e. 2¹⁶).

- * Ranges from 49,152 to 65,535 (i.e. 2¹⁶).
- * Assigned by the operating system dynamically (suppose we are browsing www.google.com from our pc/laptop then this will assign a dynamic port no to this process. As the destination port nos are very important so well-known port nos are assigned to the destinations)

*

port numbers in URLs

- * Port numbers are sometimes seen in web or other uniform resource locators (URLs).
- * By default, HTTP uses port 80 and HTTPS uses port 443.
- * URL - `http://www.example.com:8080/path/` specifies the web browser to connect to port 8080 of the HTTP server.

In application layer many processes are running simultaneously. For process-to-process delivery of data we have seen port numbers are very important. When the application layer data is passed to transport layer, the transport layer headers are appended to the data. It may be TCP (Transmission control Protocol) and UDP (User Datagram Protocol) headers depending on the information content.

Some information communication can allow some delay but cannot compromise on the reliability (i.e. data losses) and some information communication can allow some losses on the other hand cannot allow any delay.

Data link layer - communication is done using MAC addresses i.e. hardware address.

Network layer / internet layer - communication is done using IP addresses or internet protocol addresses. These are often named as software addresses.

Transport layer— communication is done using port addresses of both the source process and the destination process.

The transport layer moves

Application layer— data between applications or devices in the network

Application layer → Is the direct interface between users and data are generated & received at this layer

Two important protocols

- TCP (Reliable)

- ~~UDP~~

- No loss but delay

- e.g. → Email

- some delay can be allowed by no loss in information is not allowed

- Retransmission is not possible.

(1) HTTP (website/webbrowsers)

(2) FTP

(3) SMTP

(4) Telnet (Remote login)

- UDP (unreliable)

- No delay but loss

- Real time traffic

- Video conferencing, conferencing, live call.

- Delay may introduce chaos in the communication and retransmission is also not possible.

(1) DHCP

(Dynamic Host configuration protocol)

(2) DNS

(3) SNMP

(4) TFTP

(5) VoIP

uDP (User Datagram Protocol):-

- Simple protocol that provides the basic transport layer function.
- used by applications that can tolerate tolerate small loss of data (as no retransmission is possible)
- used by applications that cannot tolerate delay

used by:-

① DNS

② VoIP

③ SMTP SNMP (Simple Network Management Protocol)

④ DHCP

(5) TFTP (Trivial File Transfer Protocol)

(6) Online games.

→ no connection establishment between source & destination

* connectionless and unreliable.

* Prior communications (as handshaking) are not required in order to setup communication channels on data paths.

* UDP-based servers applications are assigned well-known or registered port numbers.

* UDP client process randomly selects port numbers from range of dynamic port numbers (these are operating system assigned port numbers) as the source port

* UDP is suitable for purposes where error checking and correction are either not necessary or are performed in the applications

UDP avoids the overhead of such processing in the protocol stack.

* NO error correction.

~~UDP~~ ~~UICP~~ Time-sensitive applications often use

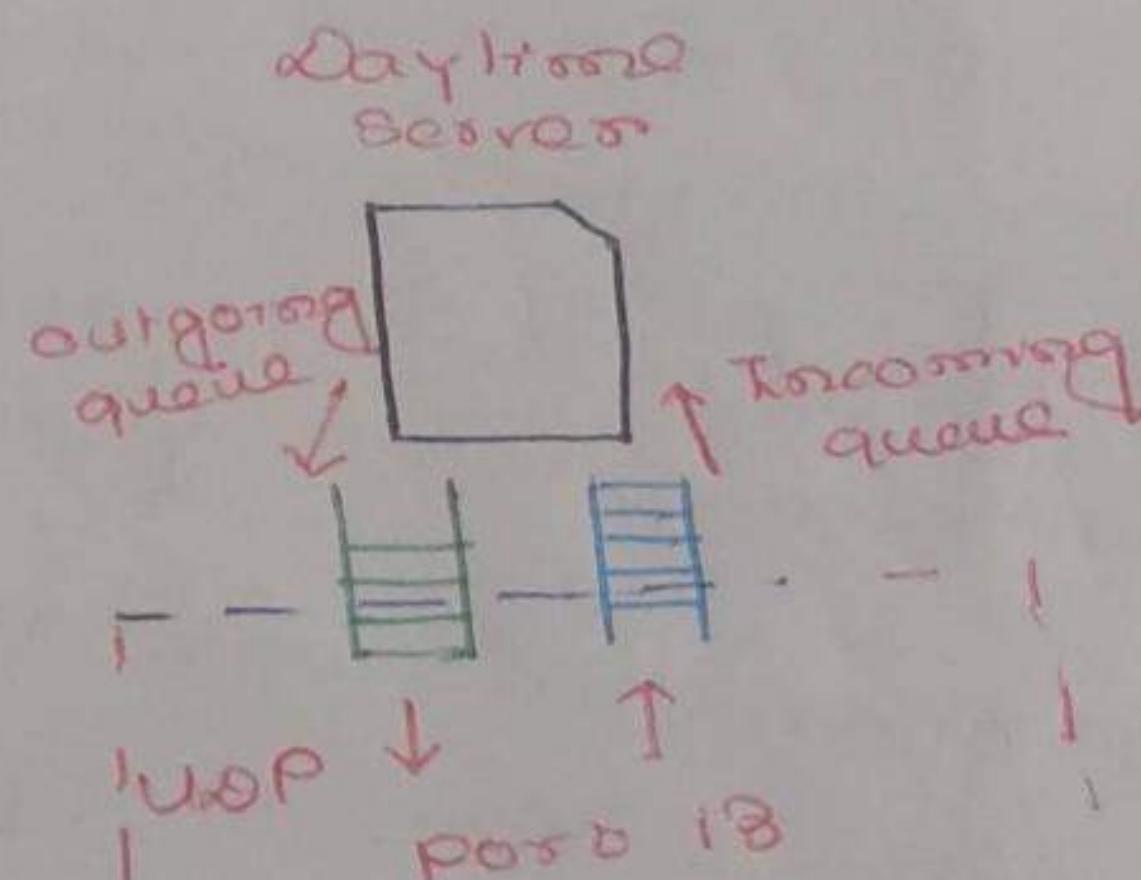
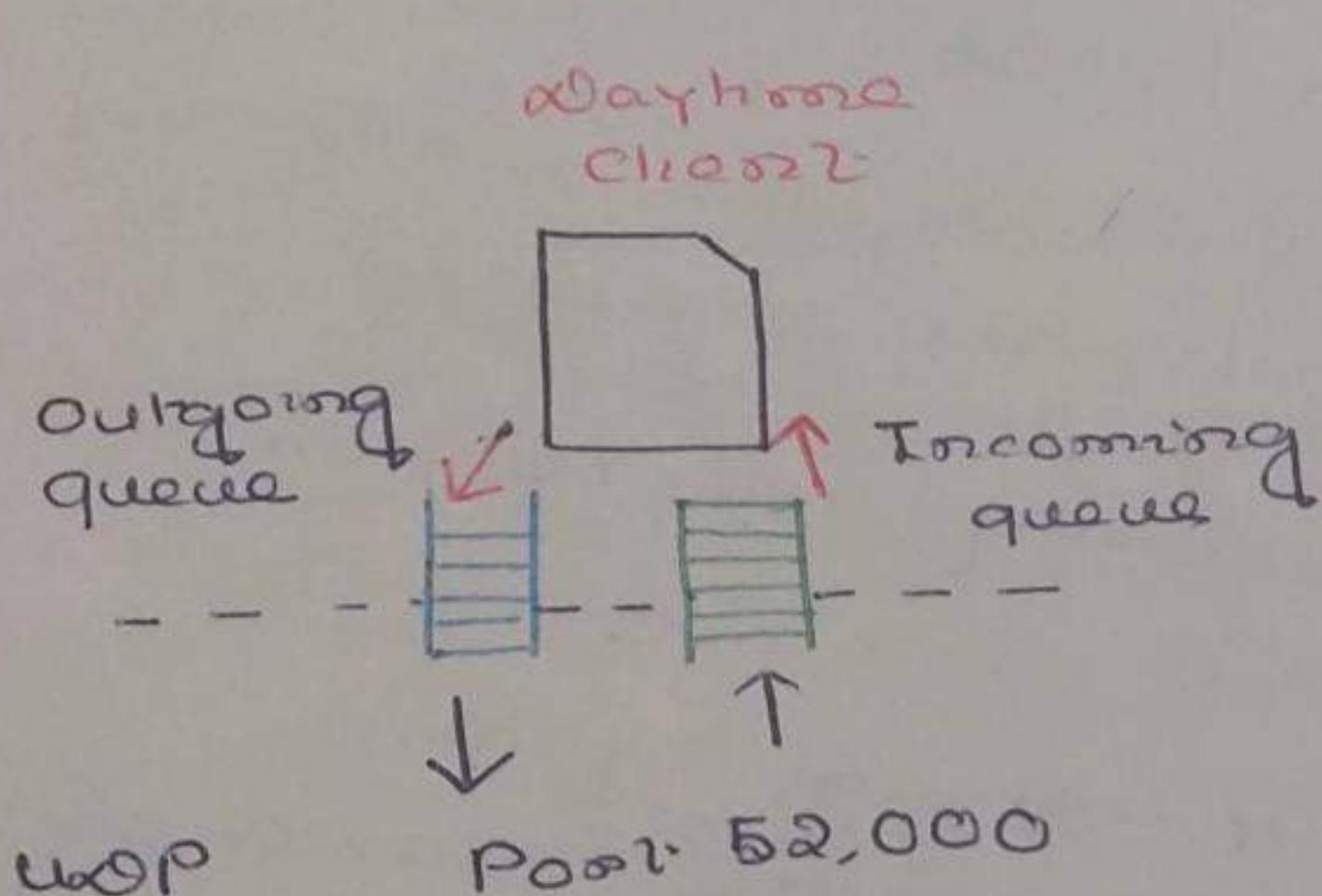
UDP because dropping packets is preferable than to waiting for packets due to retransmission which may not be an option in a real-time traffic on system.

* No Flow control mechanism.

The UDP ^{headers} packets are very simple and have only four fields. These UDP headers are kept simple because UDPs are used for real-time communication so when a source receives an UDP packet it should not take more time to process it.

* Encapsulation and Decapsulation is done by the UDP protocol.

* Queuing is done the UDP.

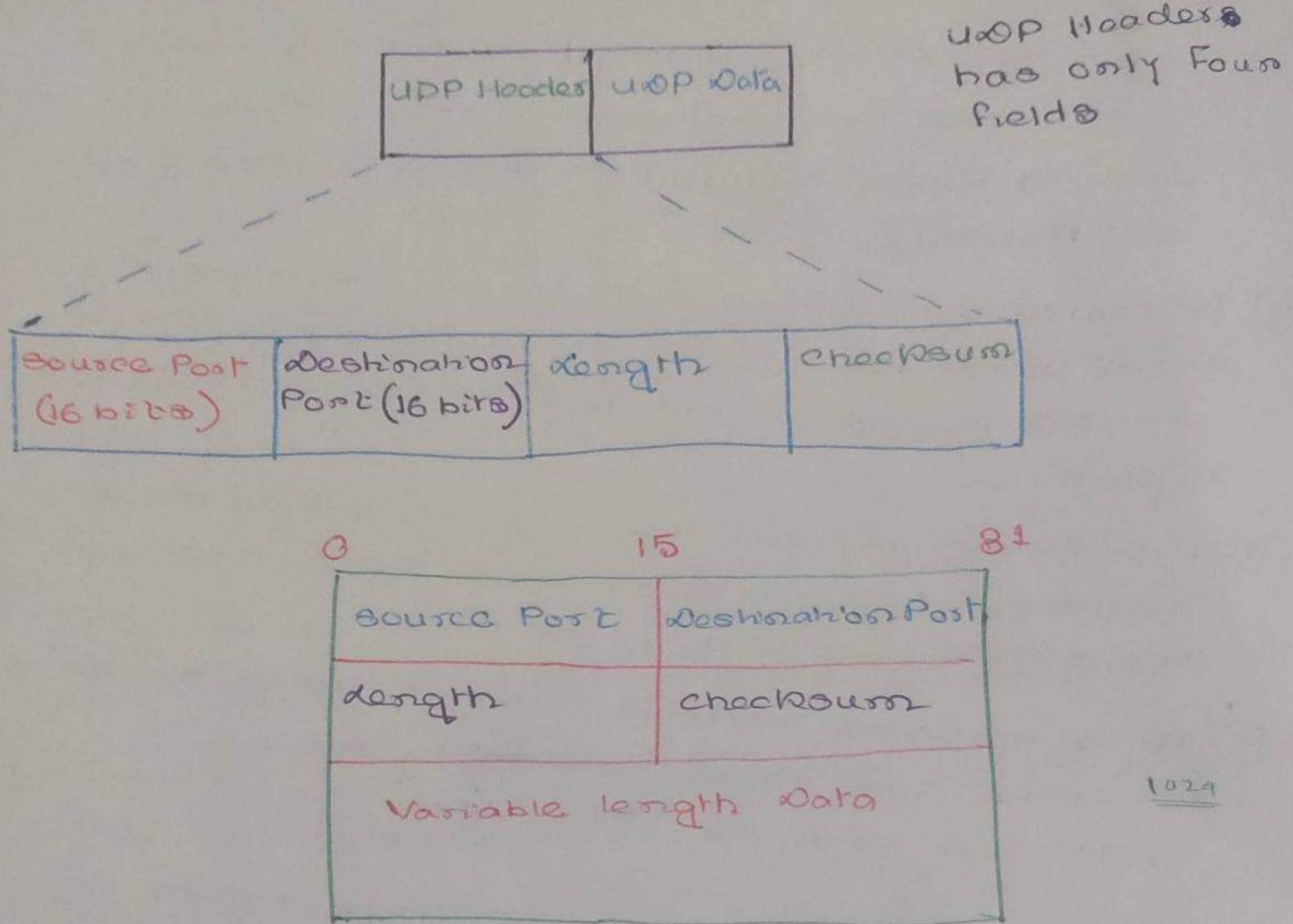


In application layer many processes are running simultaneously. If the client has two queues the server also has to maintain two queues. The UDP dequeues messages one after another and adds UDP header and passes it to the next layer i.e. network layer to add IP header. When the process are terminated at the application layer, the queues are also discarded.

USES OF UDP:-

- ① It is a transaction-oriented, suitable for simple request-response protocols such as DNS (Domain Name System) or the NTP (Network Time Protocol).
- ② It provides datagrams, suitable for modeling other protocols such as IP tunneling or remote procedure call and the Network File system.
- ③ It is simple, suitable for bootstrapping or other purposes without a full protocol stack, such as the DHCP and TFTP.
- ④ It is stateless, suitable for very large numbers of clients, such as in streaming media applications such as IPTV. (because of simplified header).
- (5) The lack of retransmission delay makes it suitable for real-time applications such as VoIP, online games, and many real-time streaming applications.
- (6) UDP is a suitable transport protocol for multicasting. Multicasting capability is embedded in the UDP software but not in the TCP software.
- (7) UDP is used for some route updating protocols as routing information protocol (RIP).

UDP Header Format :-



All the four field are of 16 bits length.

Source port Number :-

- This is the port number used by the process running on the source host. usually this port number is assigned by the operating system.
It is a 16-bit long, which means that the port number can range from 0 to $(2^{16}) - 1$ i.e. 65,535.
- If the source host is the client (a client sending a request), the port number is most cases is an ephemeral port number i.e. random port numbers greater than 1024 (well known and registered) requested by the process and chosen by the UDP software running on the source host.

- If the source host is the server (a client sending a response), the port number in most cases is a well-known port number.

Destination Port number:-

- This is the port number used by the process running on the destination host.
- It is also 16 bits long. If the destination host is the server (a client sending a request), the port number, in most cases, is a well-known port number.
- If the destination host is the client (a server sending a request response), the port number in most cases, is a ephemeral (i.e. random) port number.
- In this case, the server copies the ephemeral port number it has received in the request packet.

Length Field:-

- This is a 16-bit field that defines the total length of the user datagram, header plus data. The 16 bits can define a total length of $0\text{ to } (2^{16}-1)$ i.e. 65,535 bytes.
- However, the total length of the user datagram need to be much less because a UDP user datagram is again stored in an IP datagram with a total length of 65,535 bytes.
- $\text{UDP length} = \text{IP length} - \text{IP header's length}$

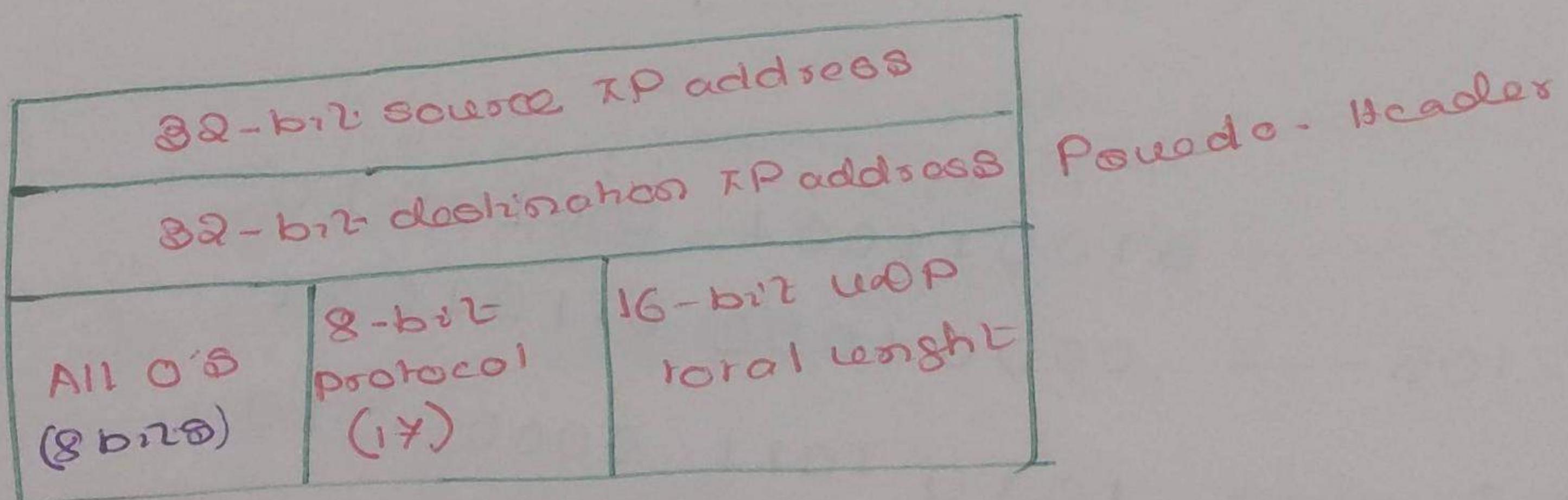
UDP checksum

Pseudo-header in UDP:-

- The UDP checksum calculation is different from one for IP and ICMP.
 - In UDP, the checksum includes three sections:
 - A Pseudo-header
 - The UDP header and
 - The data (coming from the application layer).
 - * The pseudo-header is the part of the header of the IP packet in which the user datagram is to be encapsulated with some fields filled with 0's (zeroes).
 - * If the checksum does not include the pseudo-header, a user datagram may be delivered with out errors.
 - * However, if the IP header is corrupted, it may be delivered to the wrong destination.
- The data generated by the top-most layer that is the application layer pass to the transport layer where the UDP header is encapsulated with the data. Now in the network layer along with the IP header a header field containing 0's is

added at the IPV4 field filled with 0's which is called as Pseudo-header.

- The protocol field is added to ensure that the packet belongs to UDP and not to other transport layer protocols.
- The value of the protocol field for UDP is 17. If the value is changed during transmission, the checksum calculation at the receiver will detect it and UDP drops the packet and will not deliver to the wrong destination.



Source Port Address (16 bits)	Destination Port Address (16 bits)
UDP total length (16 bits)	Checksum 16 bits
Variable length data	

UDP Header

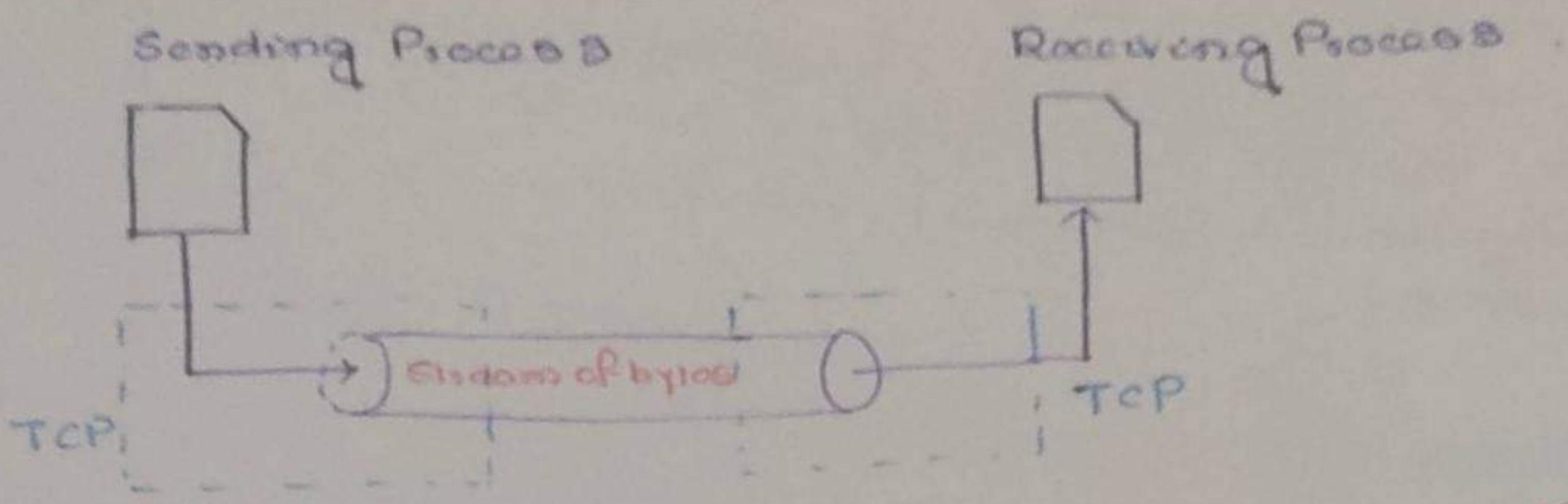
TCP (Transmission control protocol) :-

- TCP is the widely used Transport layer protocol.
- It creates a virtual connection between two TCPs to send data.
- In addition, TCP uses flow and error control mechanisms at the transport level.
- Used by applications that can tolerate delay but cannot tolerate loss.
- Used by proto applications such as:
 - ① HTTP
 - ② FTP
 - ③ Telnet
 - ④ SMTP
 - ⑤ World wide web (www)

Features of TCP

- TCP is a connection oriented protocol. Connection is established using three way handshaking before starting the communication.
- Reliable delivery (sender will know receiver has received the data or retransmission will be done)
- Acknowledgment oriented.
- Retransmission.
- Flow control (Speed control mechanism)
- Error control
- Congestion control
- Segmentation and Reassembly
- Full Duplex Support.

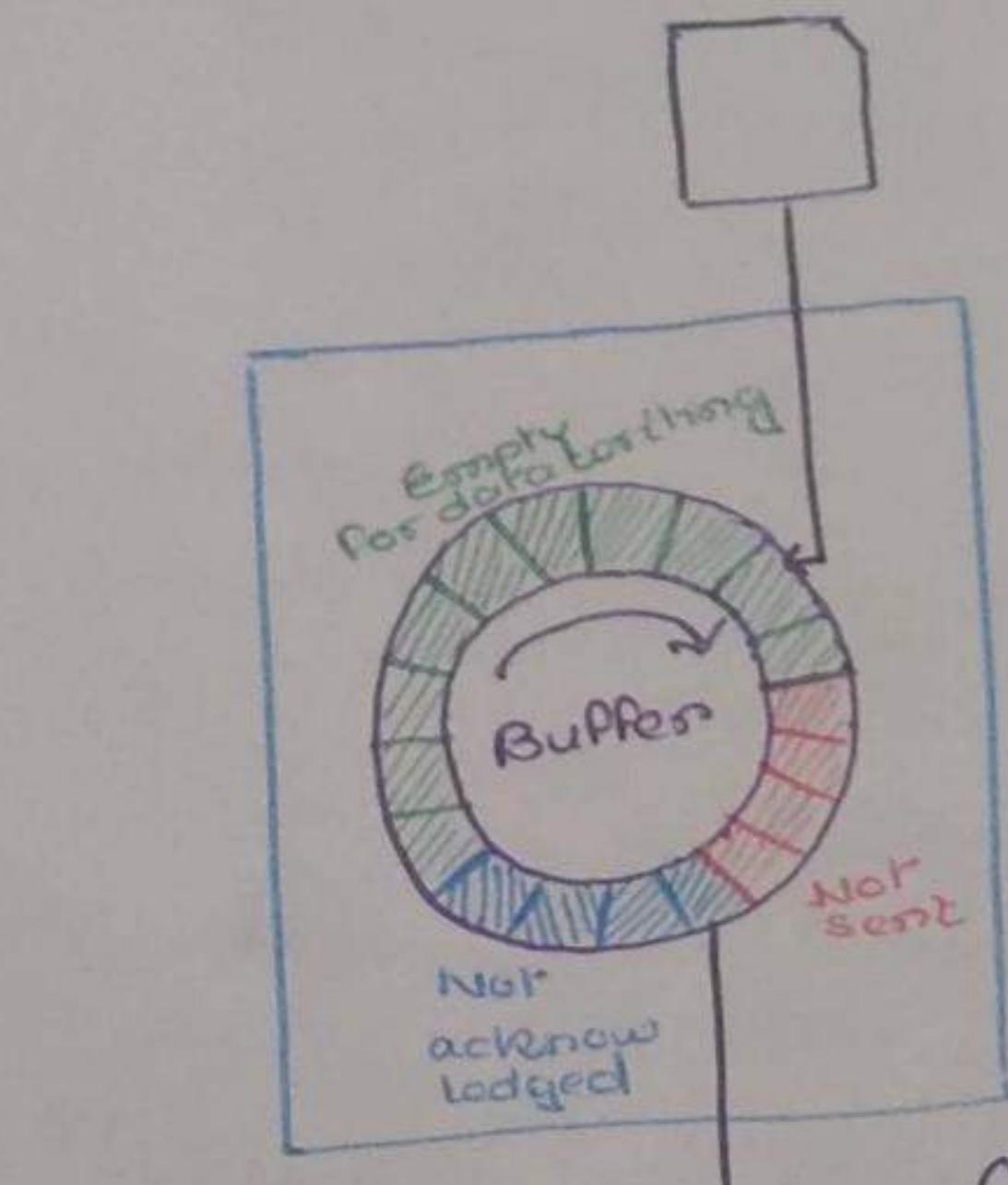
TCP Stream delivery:-



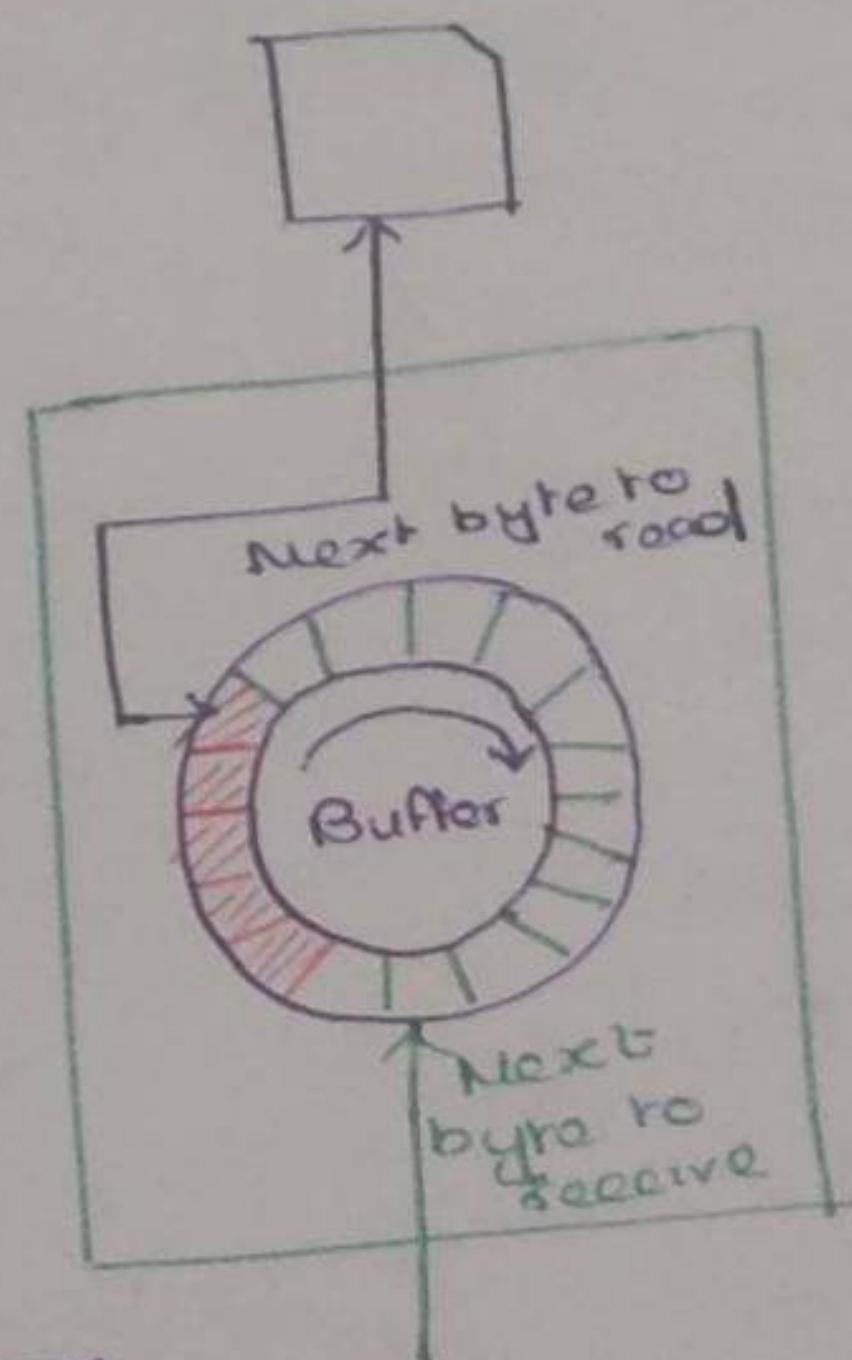
This sending and receiving process are running in two different system (e.g. computer/laptop/cellphones). This imaginary tube will deliver the data in form of stream of bytes.

TCP sending and Receiving Buffer:-

Sending Process



Receiving Process



- Red color indicated data bytes which are not sent.

- Blue cells indicate data sent by not acknowledged

- Green indicated empty buffer where data will be stored

"After acknowledgement"

received the data, chambers will be recycled.

TCP segments:-

Each segment can be of different lengths.
Each segment carries hundred or thousand of bytes. The TCP adds TCP headers to each of the segment for control and error detection activities.

Application layer generates data



This data is passed to the transport layer

The transport layer add TCP headers and make segments consists of data stream bytes of data bytes. Transport layer user datagrams are called segment



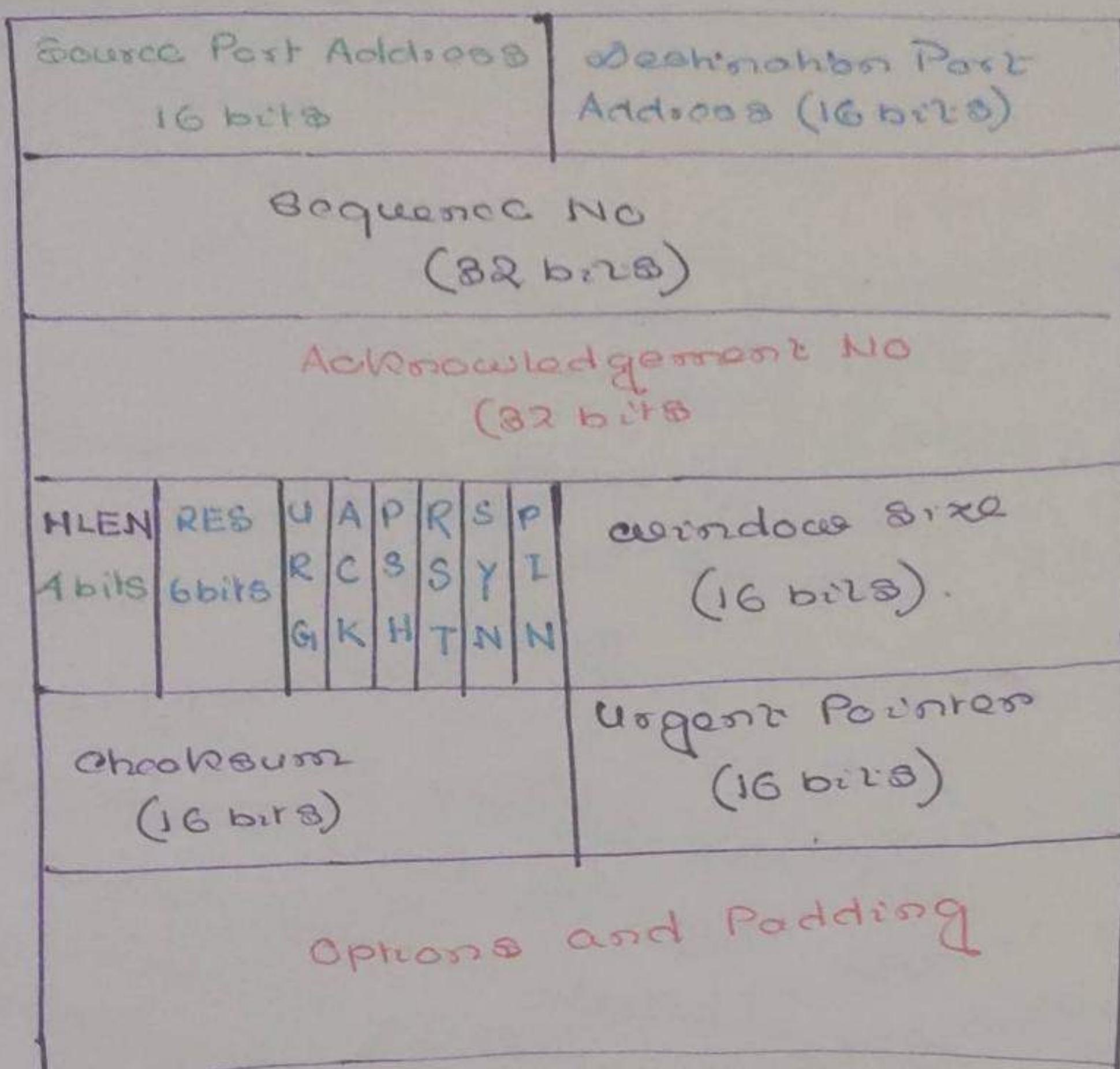
The segments will be passed to the network layer. And in this layer IP headers will be embedded to the segments. These network layer datagrams are called IP packets. If TCP headers are added then it is called segment. In UDP headers are also added.

The IP packets are then sent to the data link layer for transmission. In this layer the communication work can be done on wireless. The data link layer will add their header to the IP packets received from the network layer, and will make a frame.



This will be pass to the physical layer and this layer will convert the received frames from the data link layer to electromagnetic signals on optical signals. The physical layer protocol data units are called bits.

TCP Header Format :-



if options are added than 60 bytes

The TCP header length is 20 bytes (minimum Header).
 The TCP header plus options and padding length can go upto 60 bytes, i.e. The options and padding length can maximum go upto $(60 - 20) = 40$ bytes.

We have seen that the UDP has only 1-fields, whereas TCP/IP has more no. of fields.
 As TCP provides a reliable and acknowledgement oriented communication with error control and flow control mechanism.

Source Port Number:-

(1) It defines the port number of the application program in the host device that is sending the segment. We have seen in a client host many processes are running simultaneously. The process which is sending/requesting the data, this port number is associated with the process.

(2) This serves the same purpose as the source port address in the UDP header.

Destination Port address:-

- (1) It defines the port number of the application program in the host that is receiving the segment (well known port numbers).
- (2) This serves the same purpose as the destination port address in the UDP header.

Sequence Number:-

This is a 32-bit field that defines the number assigned to the first byte of data contained in the segment. This sequence number helps us to know about missing packets, lost packets, out of order and delayed packets.

Has a dual role:-

- If the SYN flag is set to 1, then this is the initial sequence number. The sequence number of the actual first data byte and the acknowledged number is the corresponding ACK are then this sequence number plus 1.
- Suppose the sequence number of the first data byte is 1001 then the acknowledgment (ACK) number sent by the receiver is 1002 i.e. the receiver is expecting the second data byte.
- If the SYN flag is 0, then this is the accumulated sequence no. of the first data bytes of this segment for the current session.

Acknowledgment number:-

- (1) Thus is a 32 bit field.
- (2) It defines the byte number that the receiver of the segment is expecting to receive from the other party.
- (3) If the receiver of the segment has successfully received byte numbers x from the other party it defines $(x+1)$ as the acknowledgement number. Acknowledgments and data can be piggybacked together.

hlen (Header length):-

- It indicates the number 4-byte words in the TCP header.
- The length of headers can be 20 bytes to 60 bytes i.e. $(60 - 20 = 40)$ bytes vs options & padding
- Therefore, the value of this field can be between 20 bytes i.e. $(5 \times 4 = 20)$ to 60 bytes i.e. $(15 \times 4 = 60)$. As the hlen field contains 4-byte words.

RES (Reserved field)

- It is a 6-bit field.
- It is reserved for future use and usually filled with 0's.

(e) Flag bits in TCP header:-

U	A	P	P	S	F
R	C	S	S	Y	I
G	K	H	T	N	N

(i) Fields
Flag bits are consists of 6 different control bits
on Flags each of the 6 flags are of 1 bit.
One or more of these bits can be set at a time.

(2) URG (1 bit):- when this is set v.e. L the urgent pointers field hold its significance.

S ACK (1 bit):- indicates that the acknowledgement field is significant.

T PUSH (1 bit):- push function. A&R' to push the buffered data to the receiving application.

RST (1 bit):- Reset the connection.

SYN (1 bit):- synchronise sequence numbers.

FIN (1 bit):- last packet from sender.

window size :-

- This field defines the size of the window. i.e. by 10s, that the other party must maintain.
- Suppose the receiver's window is of 20 bytes. Receiver can handle 20 bytes at a time. But if the sender without knowing the receiver's window sends 50 bytes then it can only receive 20 bytes and other bytes will be discarded. So it is very important for the receiver to inform about its window size.

This field defines the size of the window.

- The length of this field is 16 bits, which means that the maximum size of the window is

$$(2^{16}-1) = 65,535 \text{ bytes.}$$

- This value is normally referred to as the receiving window (window) and is determined by the receiver.

- The sender must obey the dictation of the receiver in this case.

checksum :-

- The calculation of the checksum for TCP follows the same procedure as the one described for UDP.
- However, the inclusion of the checksum in the UDP datagram is optional (i.e. if checksum is not added by the UDP layer to calculate), whereas the inclusion of the checksum for TCP is mandatory.
- The same pseudo-header, serving the same purpose, is added to the segment for the TCP pseudo-header. The value of the protocol field is 6. (For UDP or is 17)

Urgent Pointer :-

- ① This 16-bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data.
- We have seen the real-time traffic on urgent data is normally sent by the UDP transport protocol. But in some case we want a data to be sent urgently and also maintains its reliability. Then this is used in TCP.
- This is defined as the number that must be added to the sequence number to obtain the number of the last urgent byte in the data section of the segment.

Options:-

- This field can be upto a maximum of 40 bytes. These can be upto 40 bytes of optional information in the TCP header.
- The length of this field is determined by the Data offset field. Options have up to three fields:-
 - Options - Kind (1 byte)
 - Options - length (1 byte).
 - Options - data (variable).

Padding:-

The padding is composed of zeros. The TCP header padding is used to ensure that the TCP header ends, and data begins, on a 32-bit boundary.

TCP connection:-

1. connection-oriented
2. virtual path (seq + acknowledgement).
3. Acknowledgment process
4. Retransmission of lost damaged frames
5. TCP connection - virtual or physical
6. IP - connectionless
7. Full-duplex mode
8. Approval from other party

Three phases of TCP connection

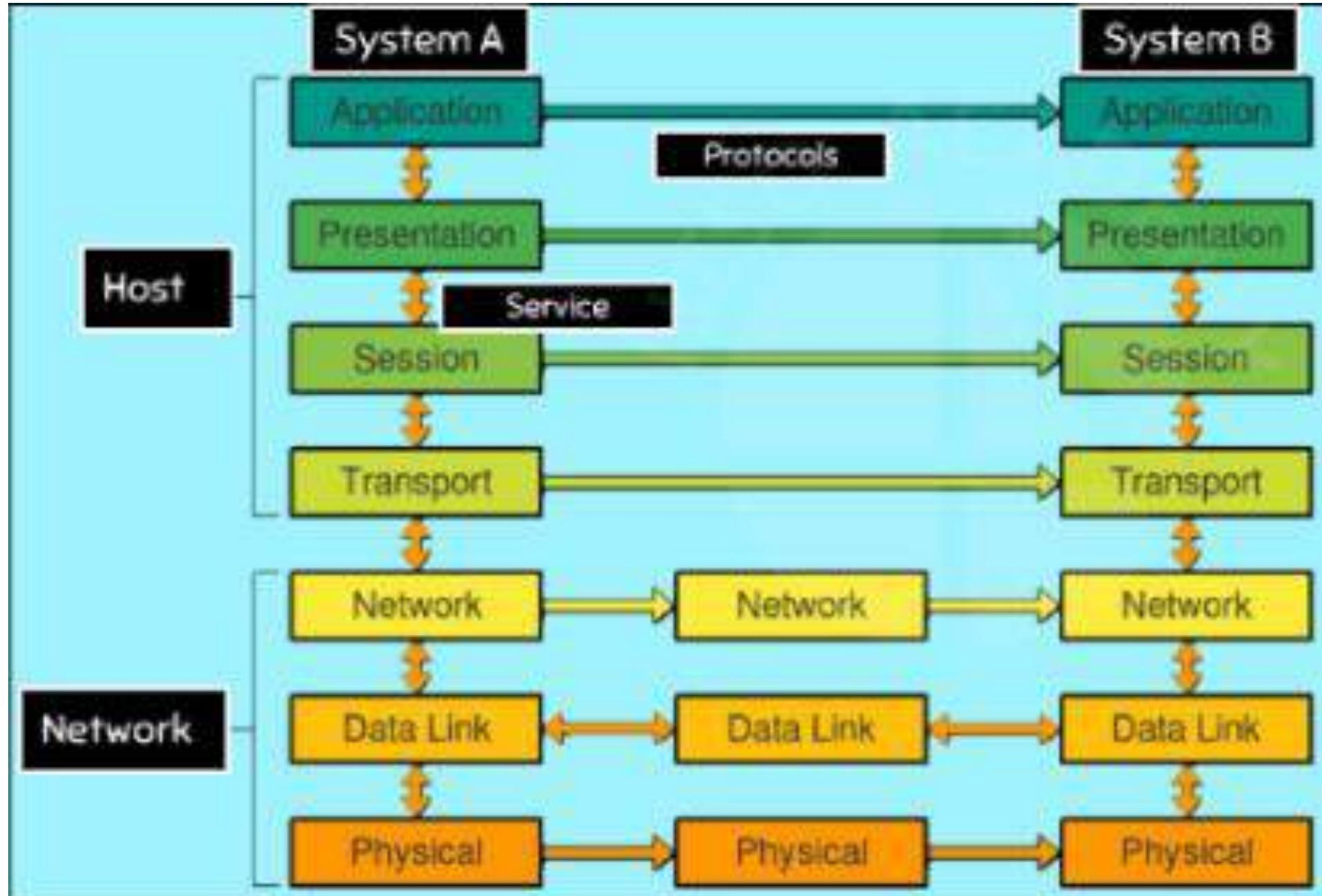
1. Connection Establishment
2. Data transfer
3. Connection Termination

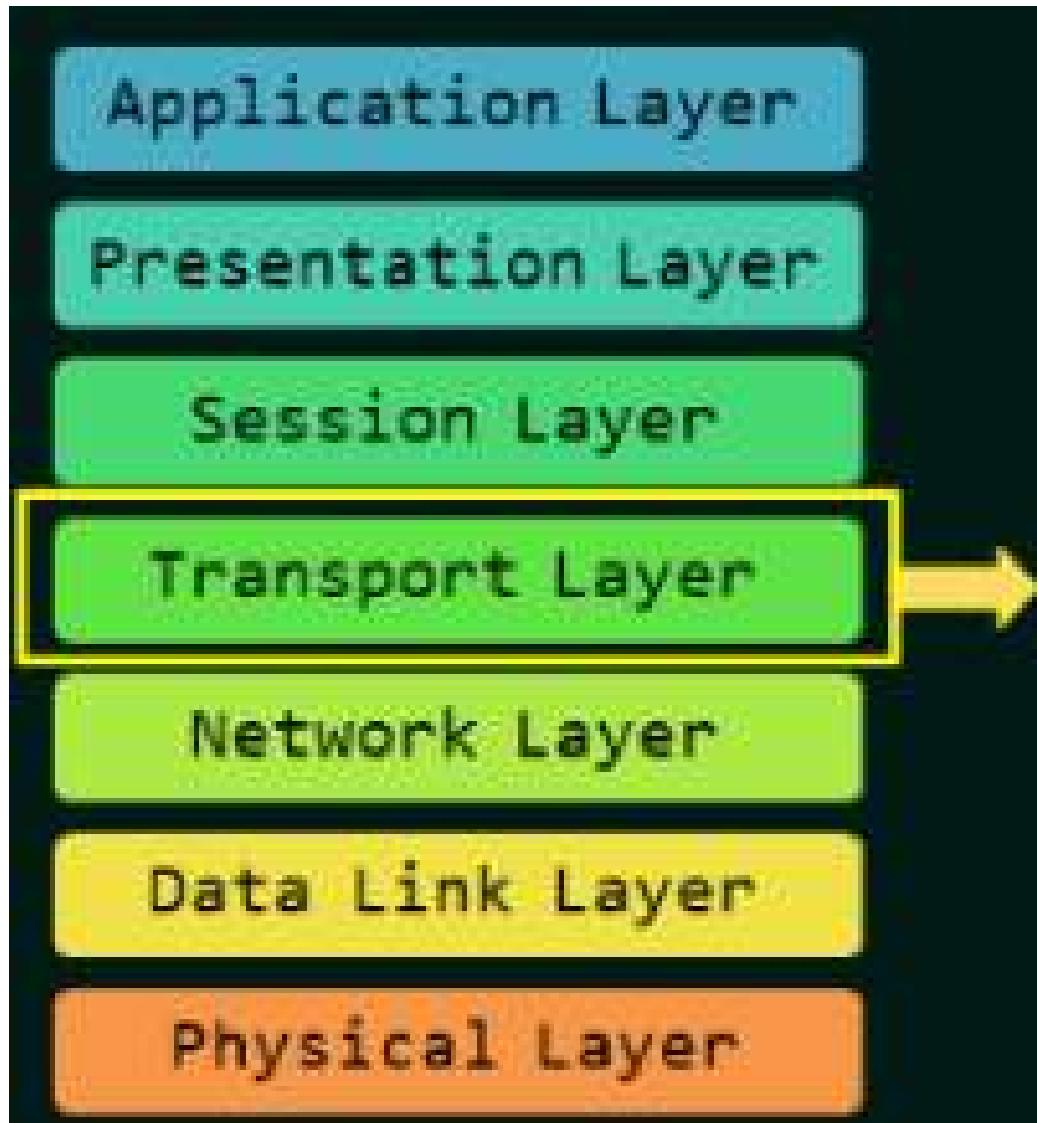
Module 4

Transport Layer



Dr. Sunandita Debnath, IIIT Vadodara



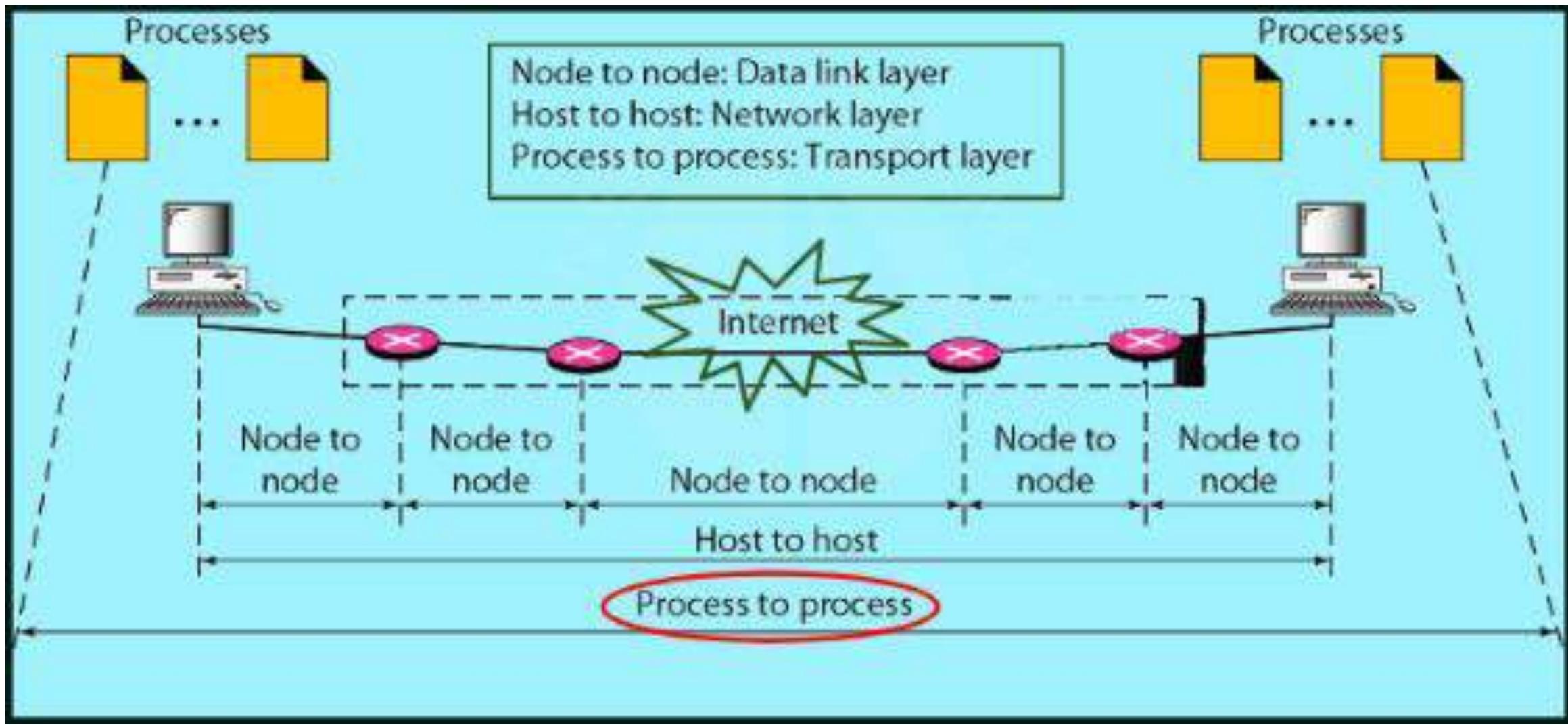


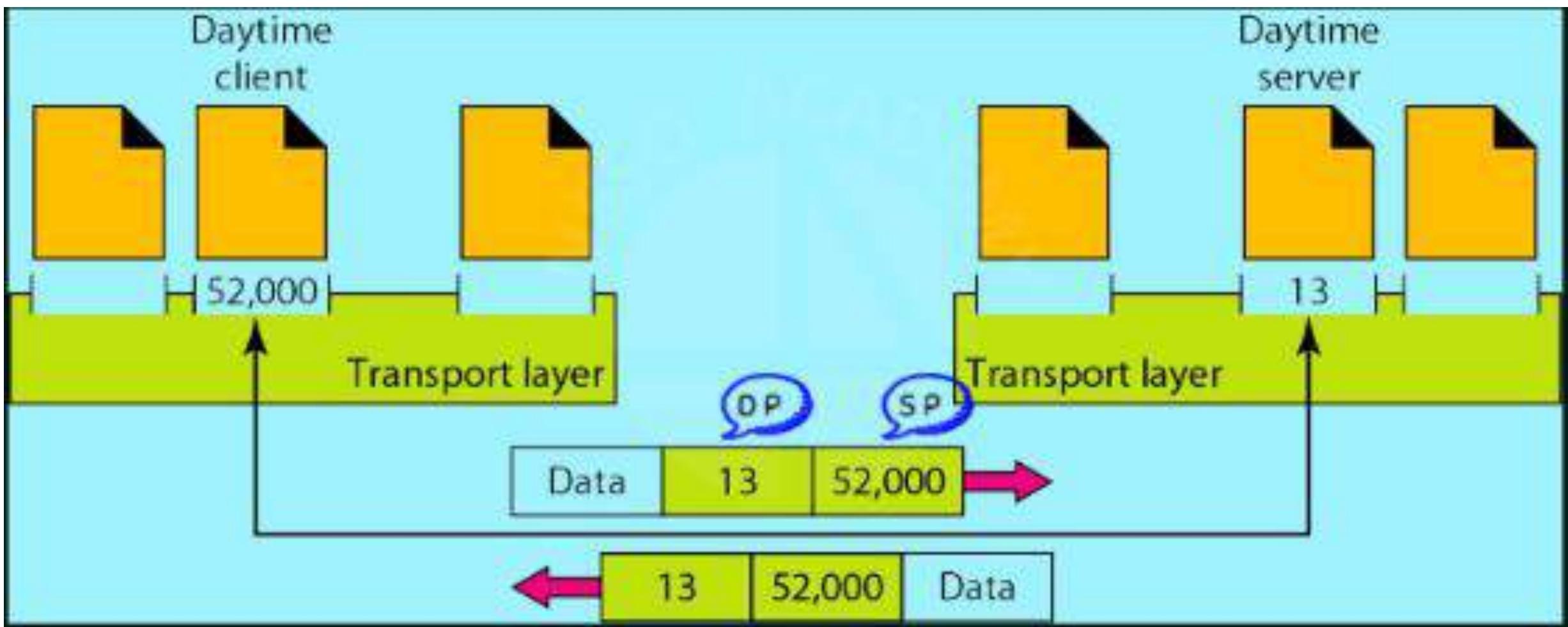
It is responsible for process to process delivery of the entire message.

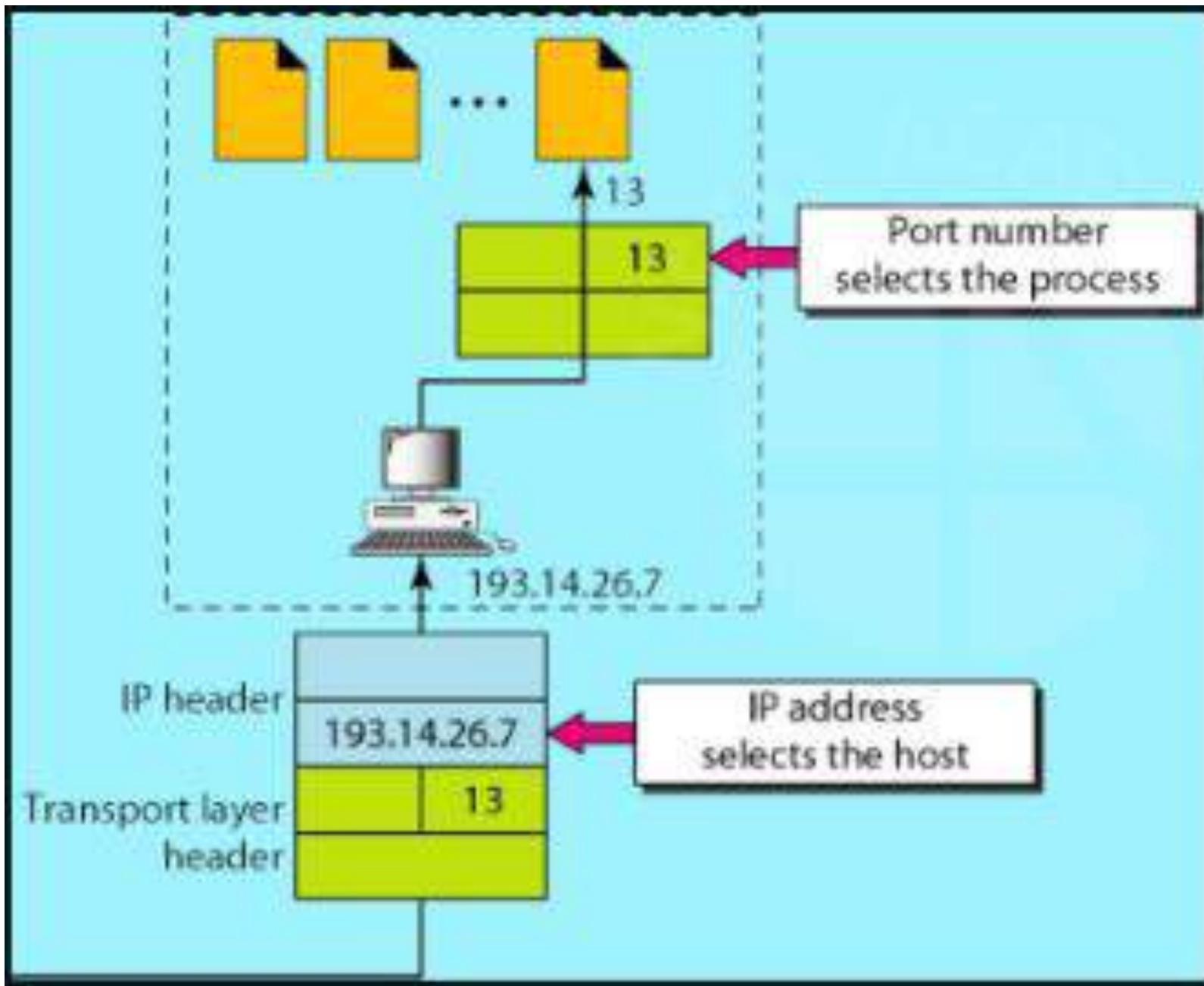
Service provided by Transport Layer

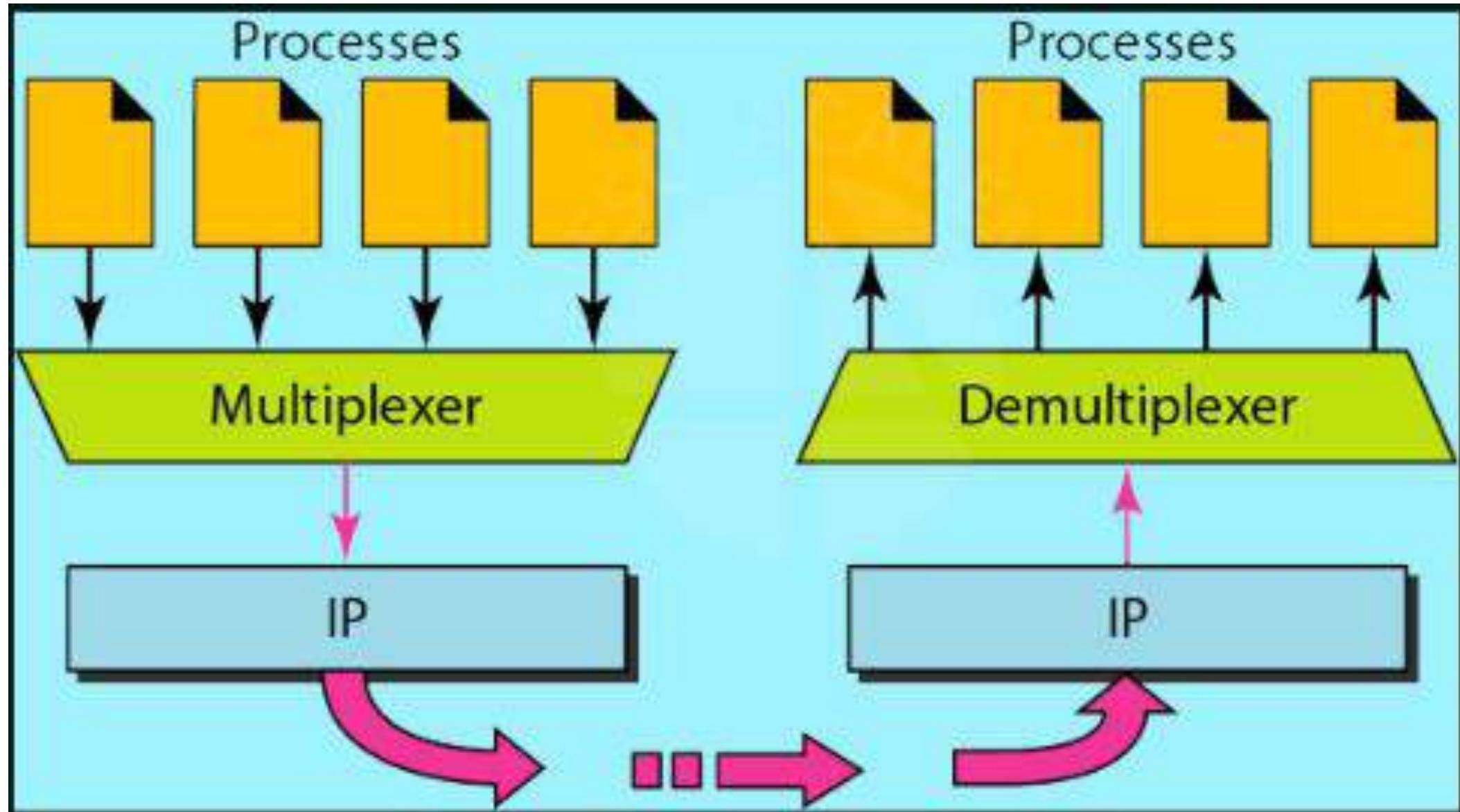
- Port addressing
- Segmentation and Reassembly
- Connection Control
- Flow control
- Error control

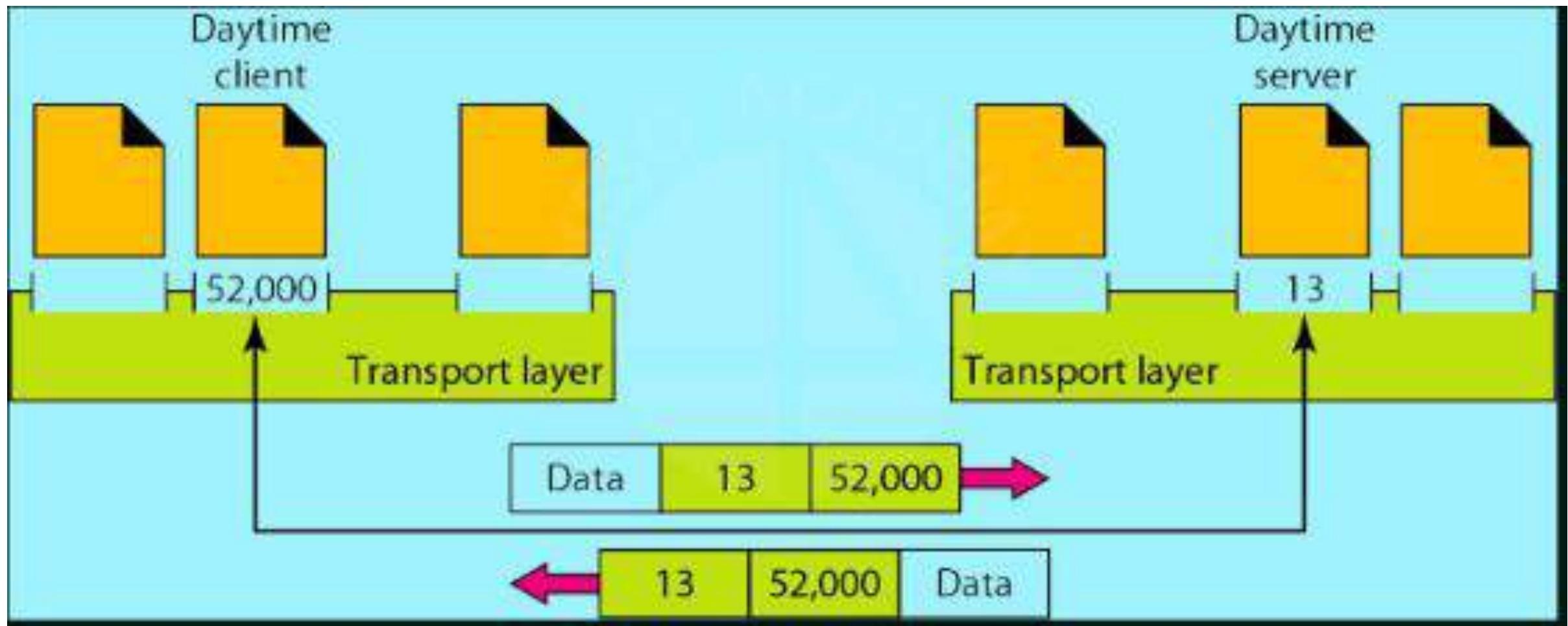




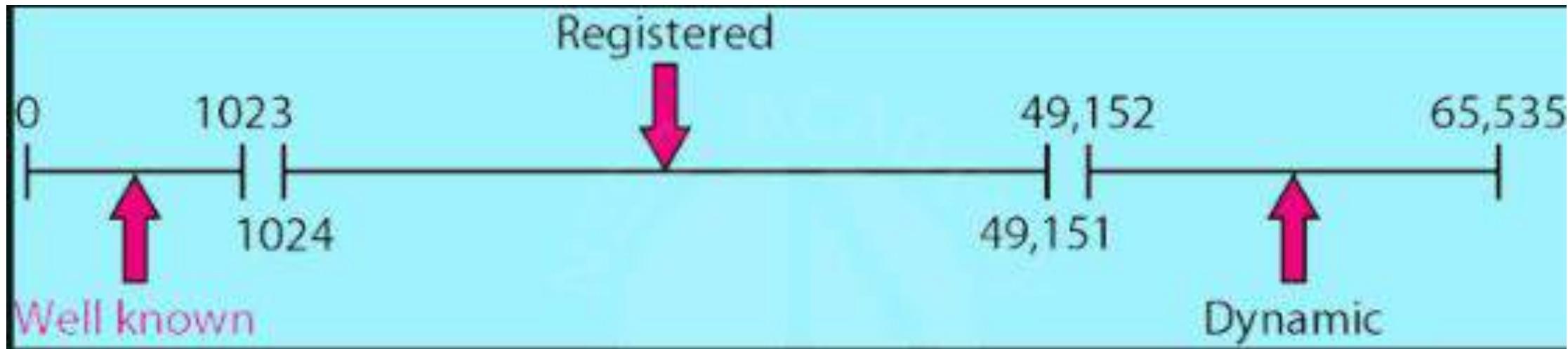








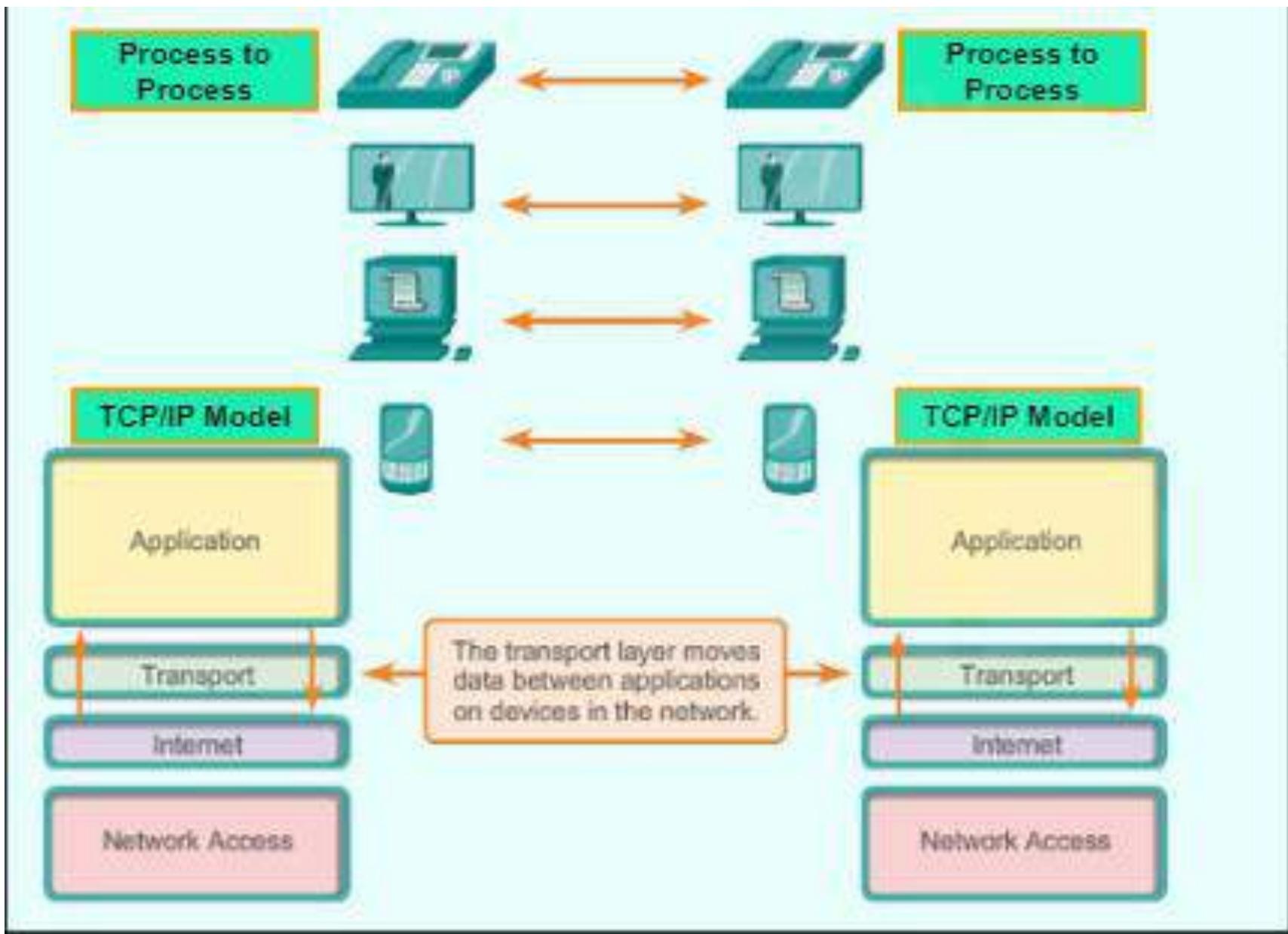
Port Numbers



- This includes the registration of commonly used port numbers for well-known Internet services.
- The port numbers are divided into three categories
 - Well-known ports
 - Registration ports
 - Dynamic or private ports

Well Known Ports

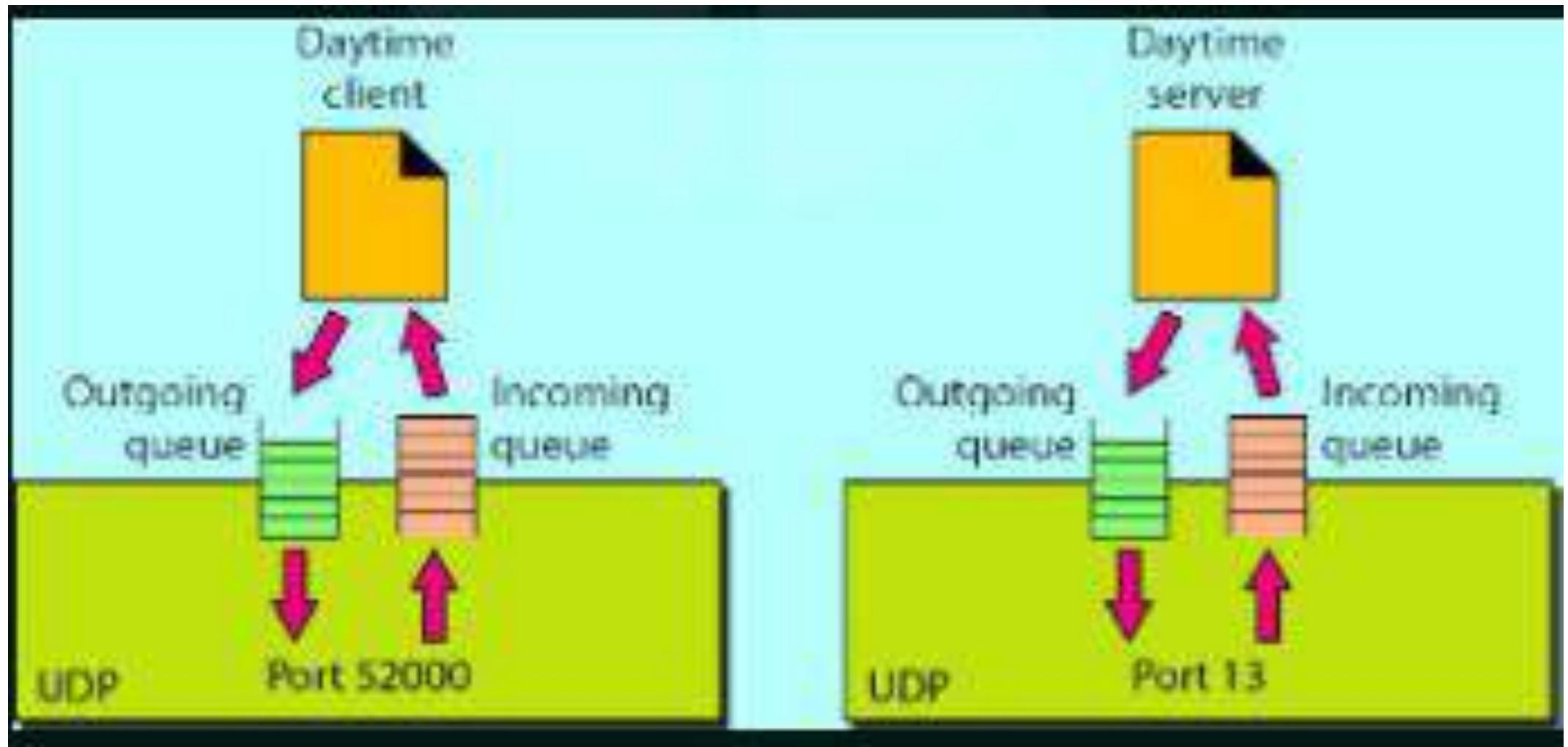
Ports Numbers	Assignments
20	File Transfer Protocol (FTP) Data Transfer
21	File Transfer Protocol (FTP) Command Control
22	Secure Shell (SSH) Secure Login
23	Telnet remote login service, unencrypted text messages
25	Simple Mail Transfer Protocol (SMTP) E-mail routing
53	Domain Name System (DNS) Service
67,68	Dynamic Host Configuration Protocol
80	Hypertext Transfer Protocol (HTTP) used in world wide web
110	Post Office Protocol (POP3)
123	Network Time Protocol (NTP)
143	Internet Message Access protocol (IMAP) Management of Digital mail
161	Simple Network Management Protocol (SNMP)
443	HTTP over SSL/ TLS (or) HTTP Secure



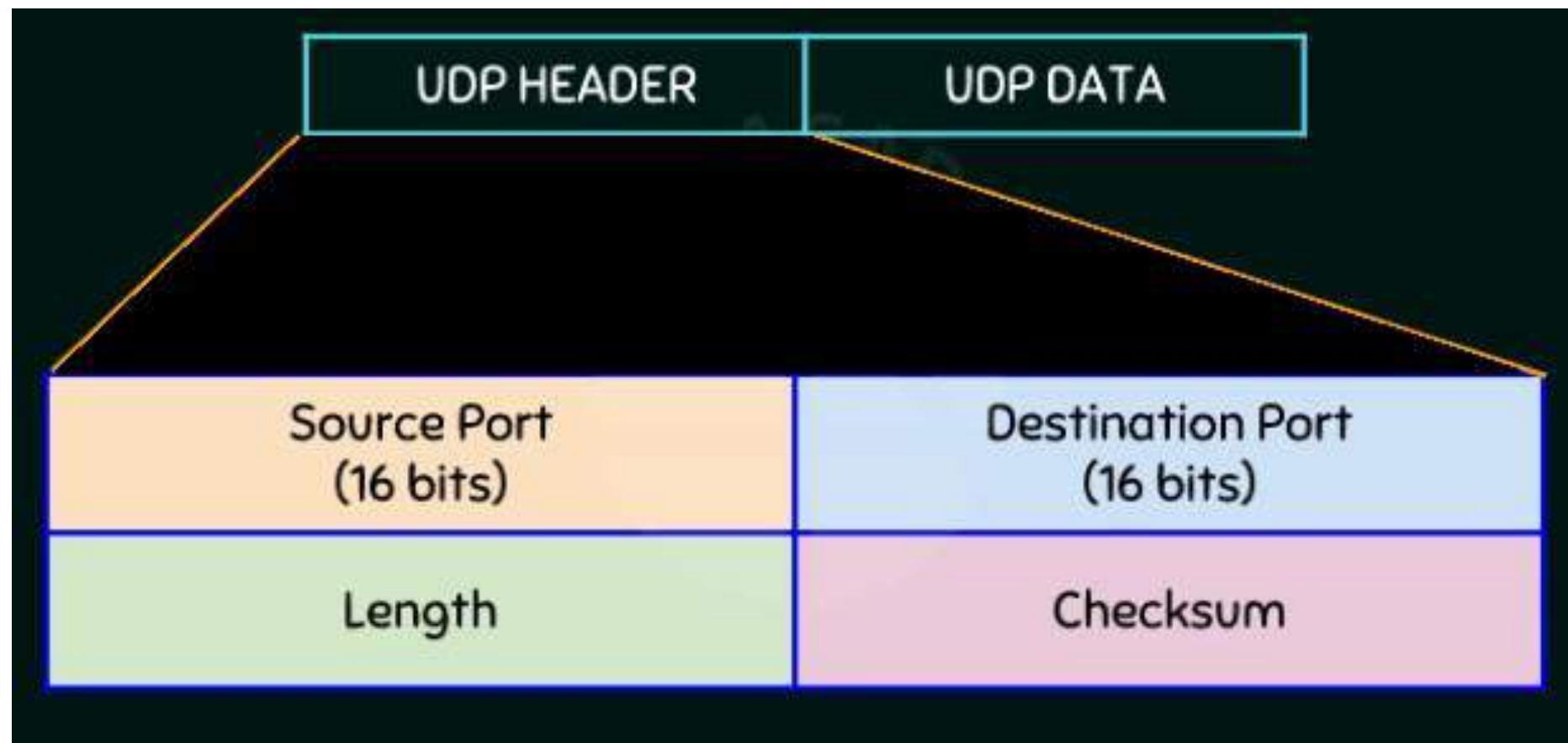
TCP (Transmission Control Protocol) vs UDP (User Datagram protocol))



TCP	UDP
<ul style="list-style-type: none">➤ No loss but delay is allowed➤ Retransmission is possible.➤ Application uses TCP as transport layer protocol<input type="checkbox"/> FTP<input type="checkbox"/> SMTP<input type="checkbox"/> HTTP<input type="checkbox"/> Telnet	<ul style="list-style-type: none">➤ No delay but low loss is allowed➤ Retransmission is not possible➤ Application uses UDP as transport layer protocol<input type="checkbox"/> DNS<input type="checkbox"/> DHCP<input type="checkbox"/> SNMP<input type="checkbox"/> TFTP<input type="checkbox"/> VoIP



UDP (User Datagram protocol) Header Format

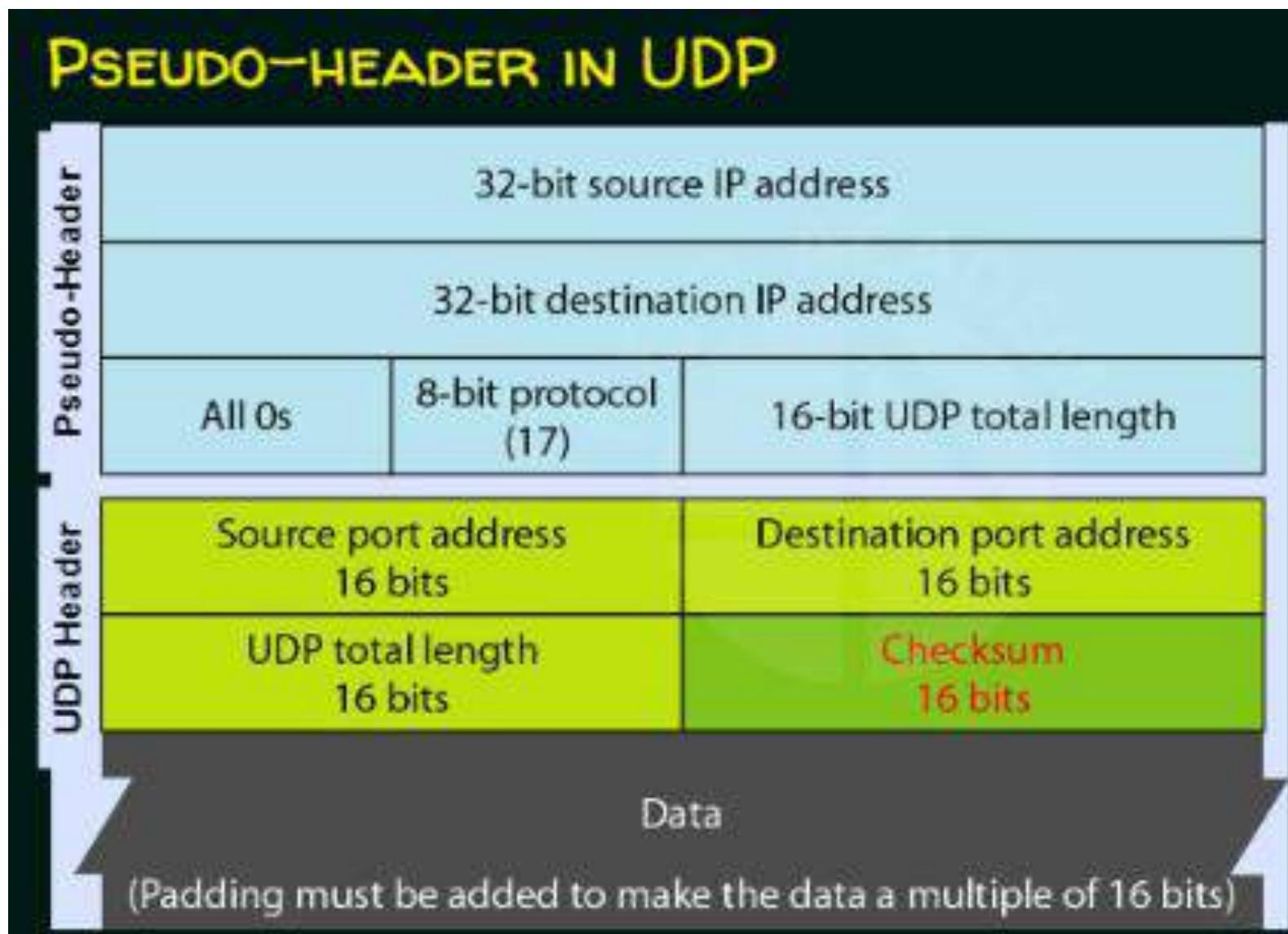


The following is a dump of a UDP header in hexadecimal format

0632000D001CE217

- a. What is the source port number?**
- b. What is the destination port number?**
- c. What is the length of the data?**
- d. What is the total length of the datagram?**
- e. Is the packet directed from a client to a server or vice versa?**

Pseudo Header in UDP (User Datagram protocol)



How to calculate Checksum in TCP Header?

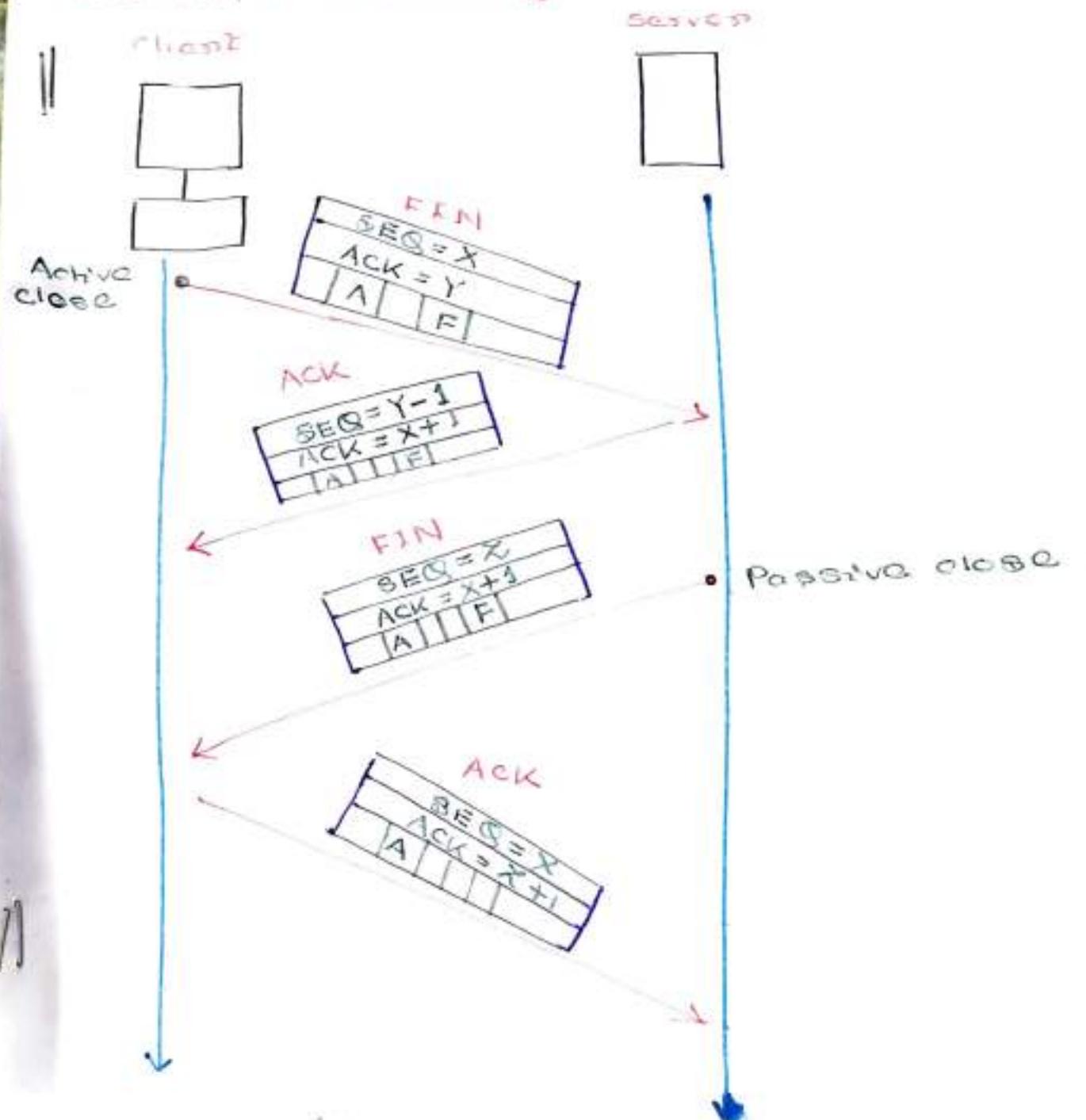
- Convert each pair composed of 16 bits into binary equivalent of the decimal. We are pairing in pair of 16 bits as the checksum value is of 16 bits.
- Same way find the ASCII values of the characters, Suppose ASCII value of T is 84, now write the equivalent binary into 8 bits format.
- Add all binary 16 bits and if carry is generated do wrapping.
- Do 1's complement of the binary value resulted from the addition. S this will give you the checksum value.

UDP (User Datagram protocol) Header Format



10011001	00010010	→ 153.18
00001000	01101001	→ 8.105
10101011	00000010	→ 171.2
00001110	00001010	→ 14.10
00000000	00010001	→ 0 and 17
00000000	00001111	→ 15
00000100	00111111	→ 1087
00000000	00001101	→ 13
00000000	00001111	→ 15
00000000	00000000	→ 0 (checksum)
01010100	01000101	→ T and E
01010011	01010100	→ S and T
01001001	01001110	→ I and N
01000111	00000000	→ G and 0 (padding)
<hr/>		
10010110 11101011		→ Sum
01101001		→ Checksum

Four way handshaking :-



Sliding windows:- window is used for flow control at the receiver.
Flow control is usually done in two layers:-

1. Transport layer.

2. Data link layer.

Now we are in Transport layer:-

Now we are in Transport layer to handle flow control.

• TCP uses a sliding window to handle flow control.

• From Go-back-N

• does not use NAK.

• The receiver holds out-of-order segments

• TCP sliding window vs

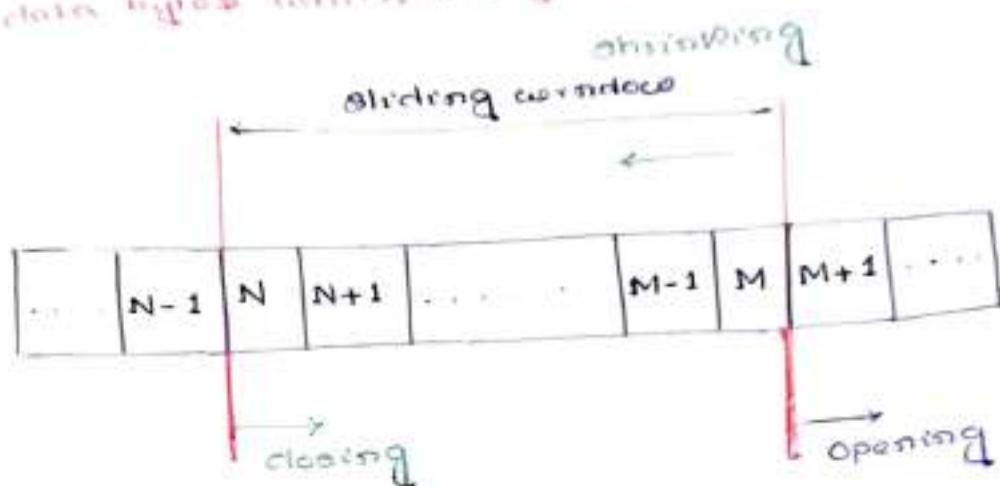
• of variable size. whereas as datalink

layer sliding window vs of fixed size.

layer sliding window vs by re-oriented.

• TCP Sliding window vs by re-oriented.
whereas datalink layer sliding window vs
of frame oriented.

- ④ the previous bytes have been acknowledged
- ⑤ the data bytes received are acknowledged immediately
- ⑥ the data bytes received are yet to sent.



window size = minimum (wind. cond)
 receiver window size congestion window size

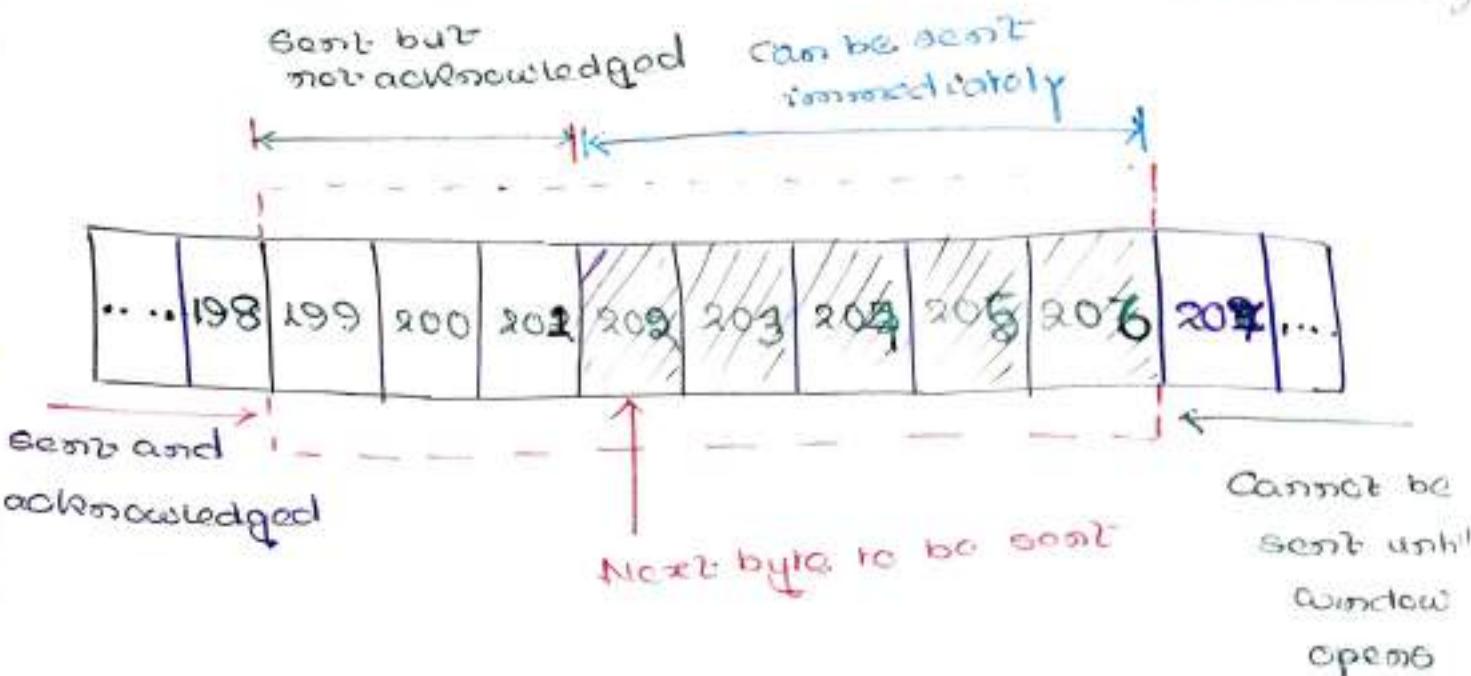
The window size is of variable length.
 The data which are sent but not have been acknowledged and the data which are to be sent immediately as will be in the window.
 Suppose the N number segment is sent and all acknowledged now the window will move towards $(N+1)$ and now the window can allow the $(M+1)$ number segment to the next segment to be sent in the queue.
 Congestion window is the per feature of intermediate devices such as router or switches. suppose the receiver has a window size of 50, but the router through which many segments of other ongoing communications are processing, so there is a congestion.

$$\text{window size} = \min(\text{round}, \text{send}) (20, 8) = 8$$

receive window size

congestion window size

(size of network window)



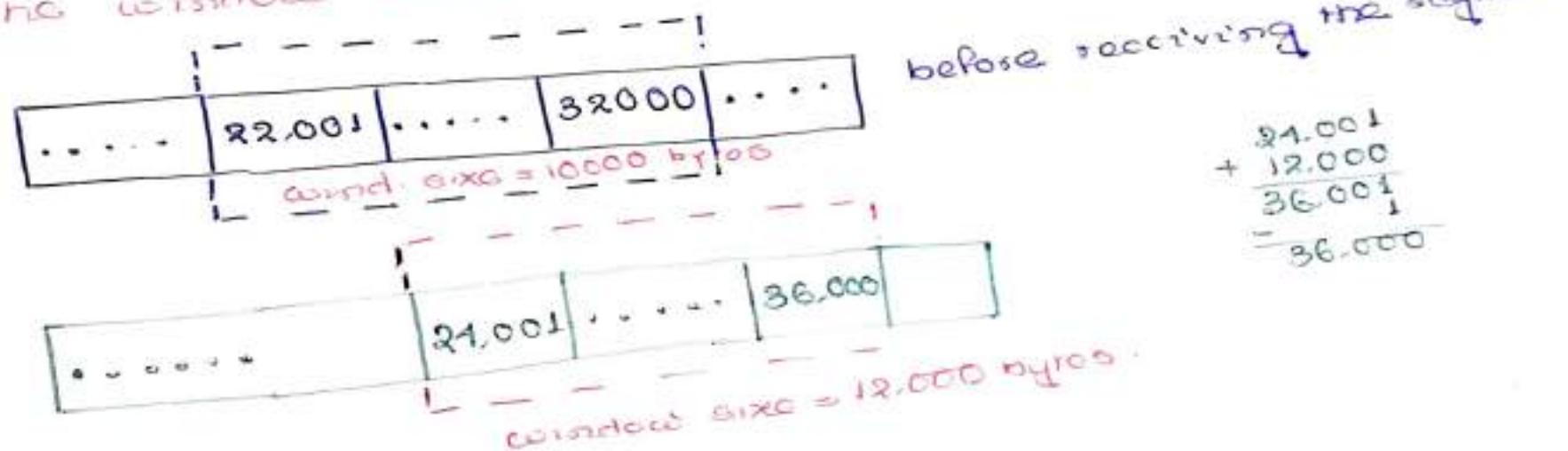
- window size \oplus = min(round, send).
- The source does not have to send a full window's worth of data.
- The window can be opened or closed by the receiver but should not be shrunk.
- The destination/receiver can send an ACK at any time.
- The sender can send 1-byte segment even after the window is shut down in the receiver side.

Q. what is the size of the window for host A if the value of send (receive window) is 3000 bytes and the value of cwnd (congestion window) is 3500 bytes?

$$\Rightarrow \text{we know, } \text{window size} = \min(\text{send}, \text{cwnd}) \\ = \min(3000, 3500) \\ = 3000 \text{ bytes}$$

Q. A TCP connection is using a window size of 10,000 bytes and the previous acknowledgement number was 22,001. It receives a segment with acknowledgement number 21,001 and window size advertisement of 19,000. Draw a diagram to show the situation of the window before and after.

$$\begin{array}{r} 22,001 \\ + 18,000 \\ \hline 32,001 \\ - 32,000 \\ \hline 0 \end{array}$$



Q. A window moves by 1000 bytes from 2001 to 5000.

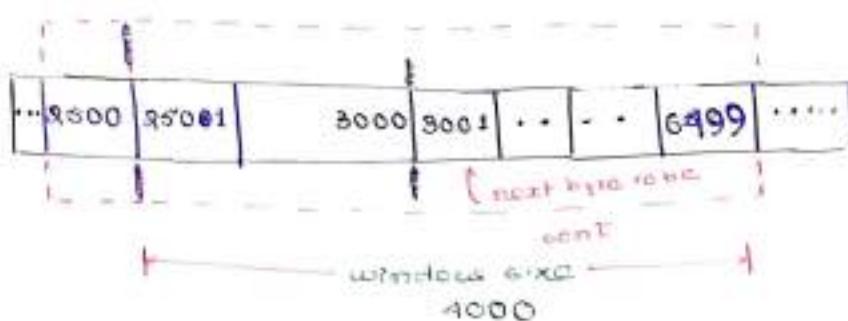
The next byte to be sent is 3001.

Figure 1 shows the situation of two events of the windows after the following two events:-

(i) An ACK segment with the acknowledgement number 2500 and window size advt. 1000 is received.

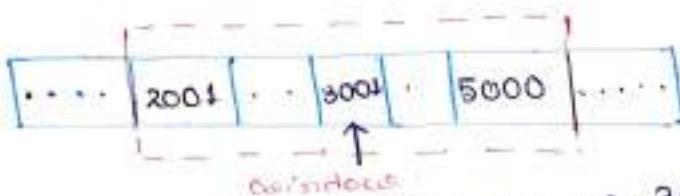
advt. 1000 is received.

(ii) A segment carrying 1000 bytes is sent.



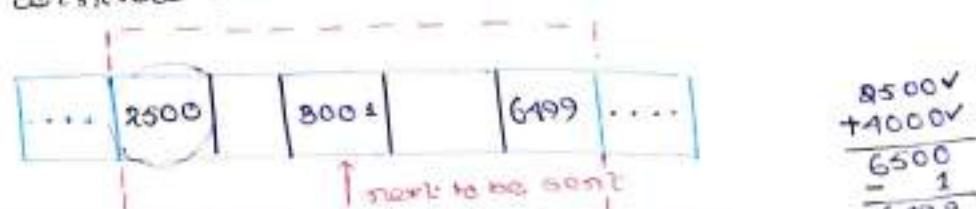
$$\begin{array}{r} 2501 \\ + 1000 \\ \hline 3501 \\ - 6500 \\ \hline 6500 \end{array}$$

Initial Figure:- The window holds bytes 2001 to 5000.

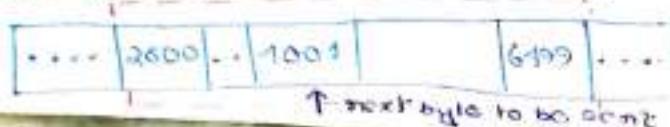


The next data byte to be sent is 3001.

An acknowledgement for 2500 is received and the new window size is 4000.



A segment carrying 1000 bytes is sent means from 3001 next 1000 bytes is sent.



From 3001 to 4000 next 1000 bytes are sent.

Transport layers

- Application → In this layer application related data is generated.
- Presentation → Here data is being compressed, encrypted
- Session → ^{red} Dialog exchange (Dialog control activities)
- Transport → It is responsible for process to process delivery of the entire message.
- Network
- Link
- Physical

Suppose at the host multiple processes are running. Suppose transport layer responsibility is to identify uniquely each host process and deliver the generated data to the intended host process. To do this each process is associated with a unique port number.

Network layer or Internet protocol layer identifies networks with these unique IP addresses. Host-to-host data delivery is done by data link layer.

MAC address — Hardware address of the devices

Services provided by Transport layer:-

1. Port addressing (Source and destination port no. are added to the data generated by the application layer and carried by the transport layer)
2. Segmentation and Reassembly
3. Connection control (connection oriented and connectionless).
4. Flow control (speed control)
5. Error control activity

Two important Transport layer protocols are

- ① TCP
- ② UDP

Transport layer

Application → In this layer application related data is generated.

Presentation → Here data is being compressed, encryption, red.

Session → Dialog exchange (dialog control activities)

Transport → It is responsible for process to process delivery of the entire message.

Network Layer

Network Layer

Physical

Suppose at the host multiple processes are running. Suppose transport layer responsibility is to identify uniquely each host process and deliver the generated data to the intended host process. To do this each process is associated with a unique port number.

Network layer or Internet protocol layer identifies networks with these unique IP addresses. Host-to-host data delivery is done by data link layer.

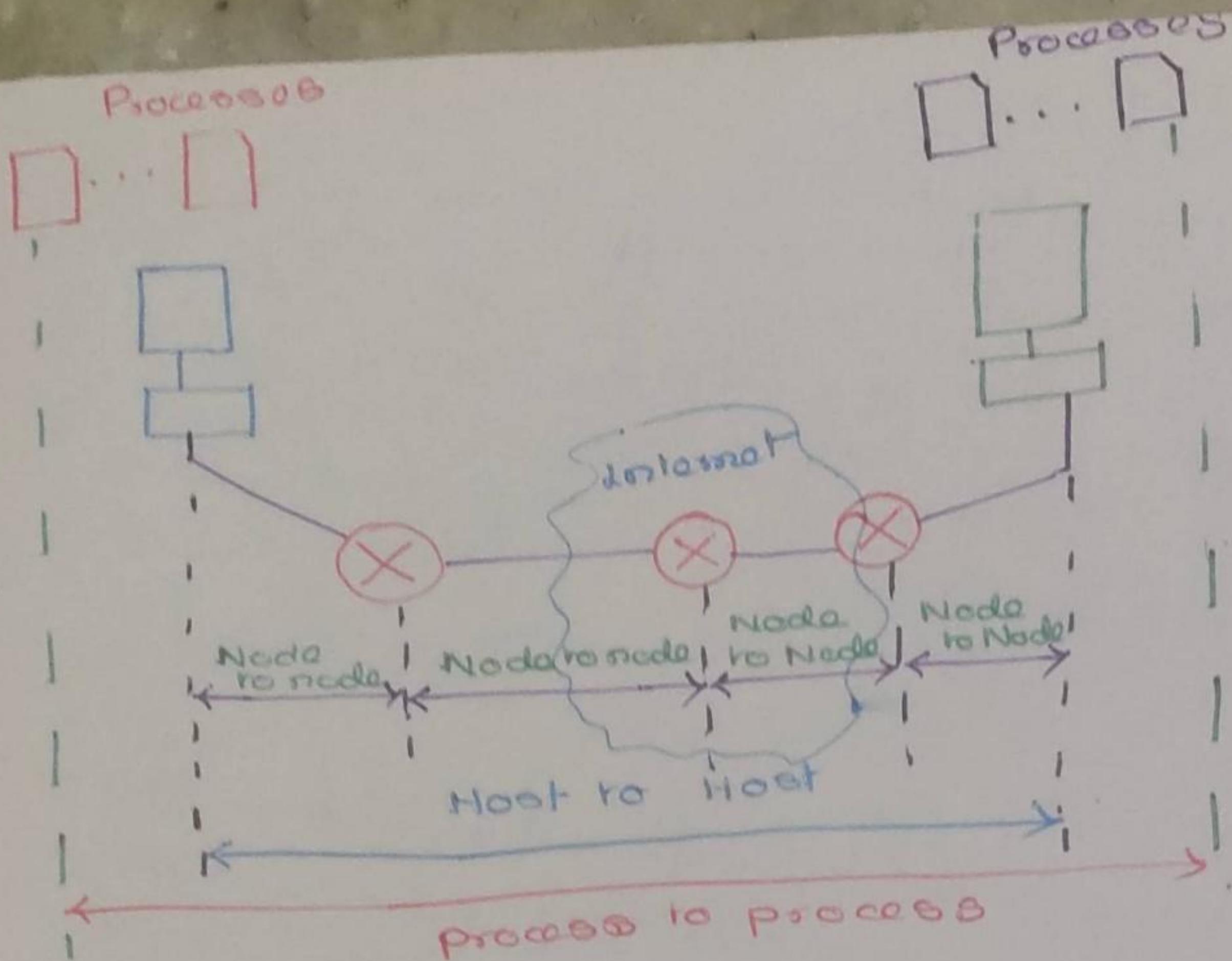
MAC address — Hardware address of the devices

Services provided by Transport layer:-

1. Port addressing (source and destination port no. are added to the data generated by the application layer and carried by the transport layer)
2. Segmentation and Reassembly
3. Connection control (connection oriented and connectionless).
4. Flow control (speed control)
5. Error control activity

Two important Transport layer protocols are

- ① TCP & ② UDP



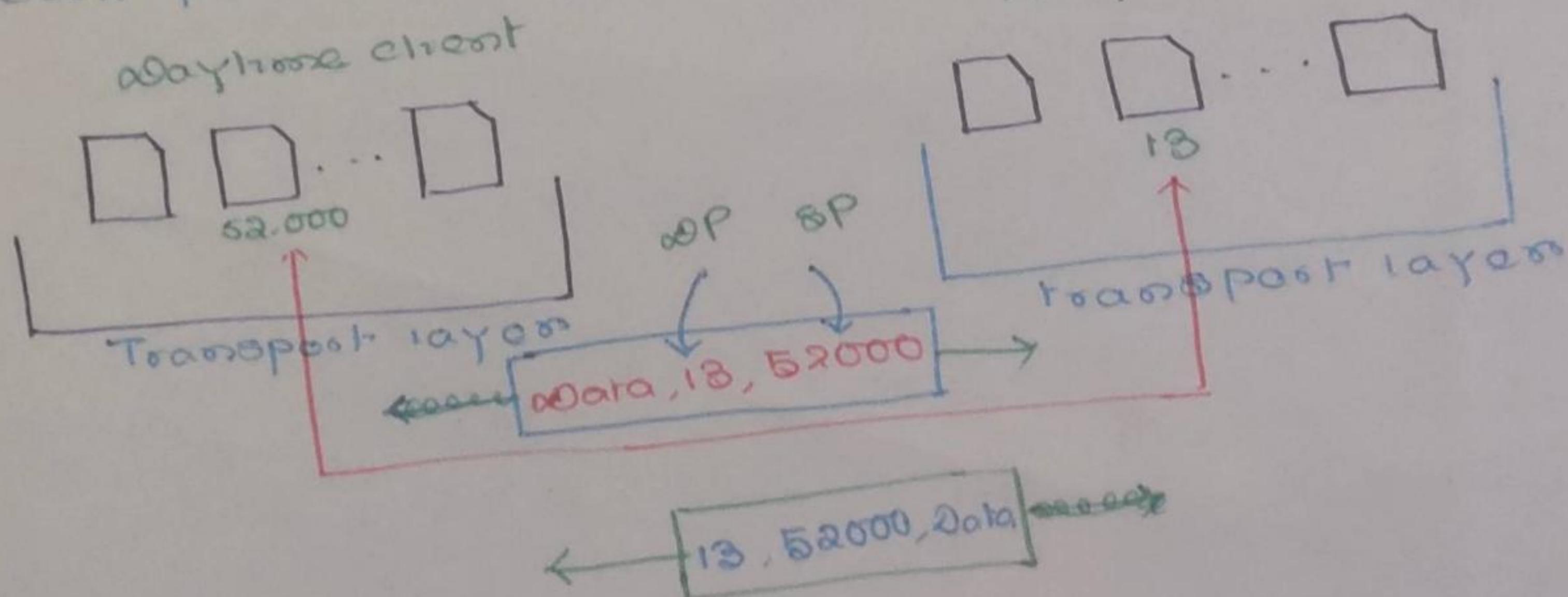
Node to Node: Data link layer (IP address)

Host to Host: Network layer (Port no.)

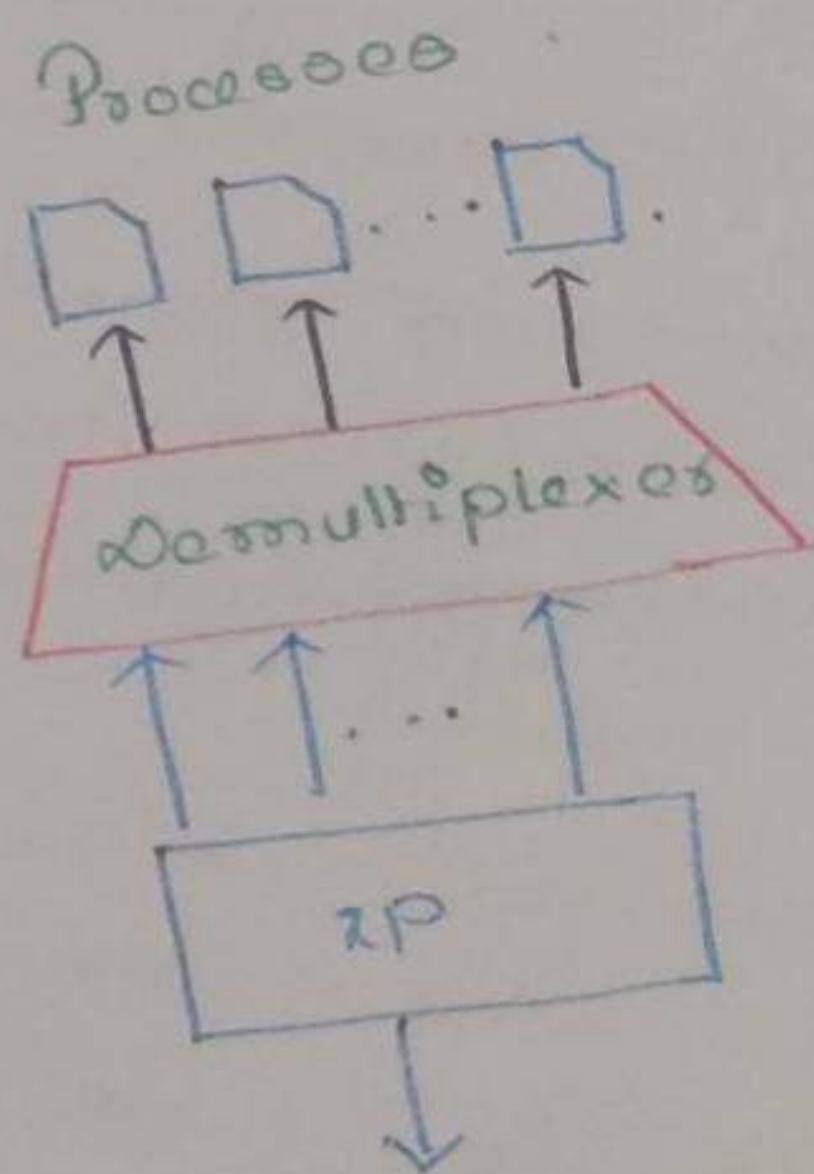
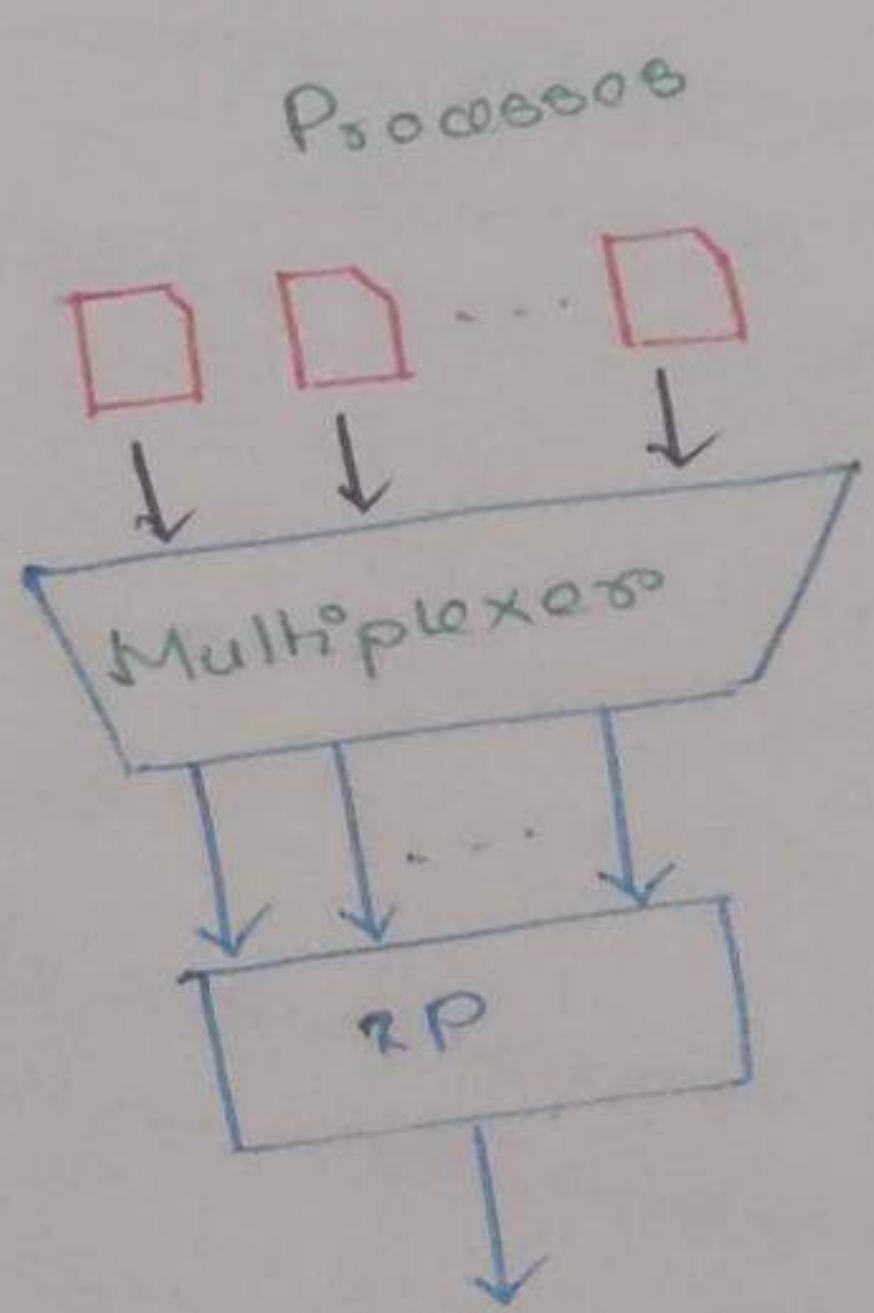
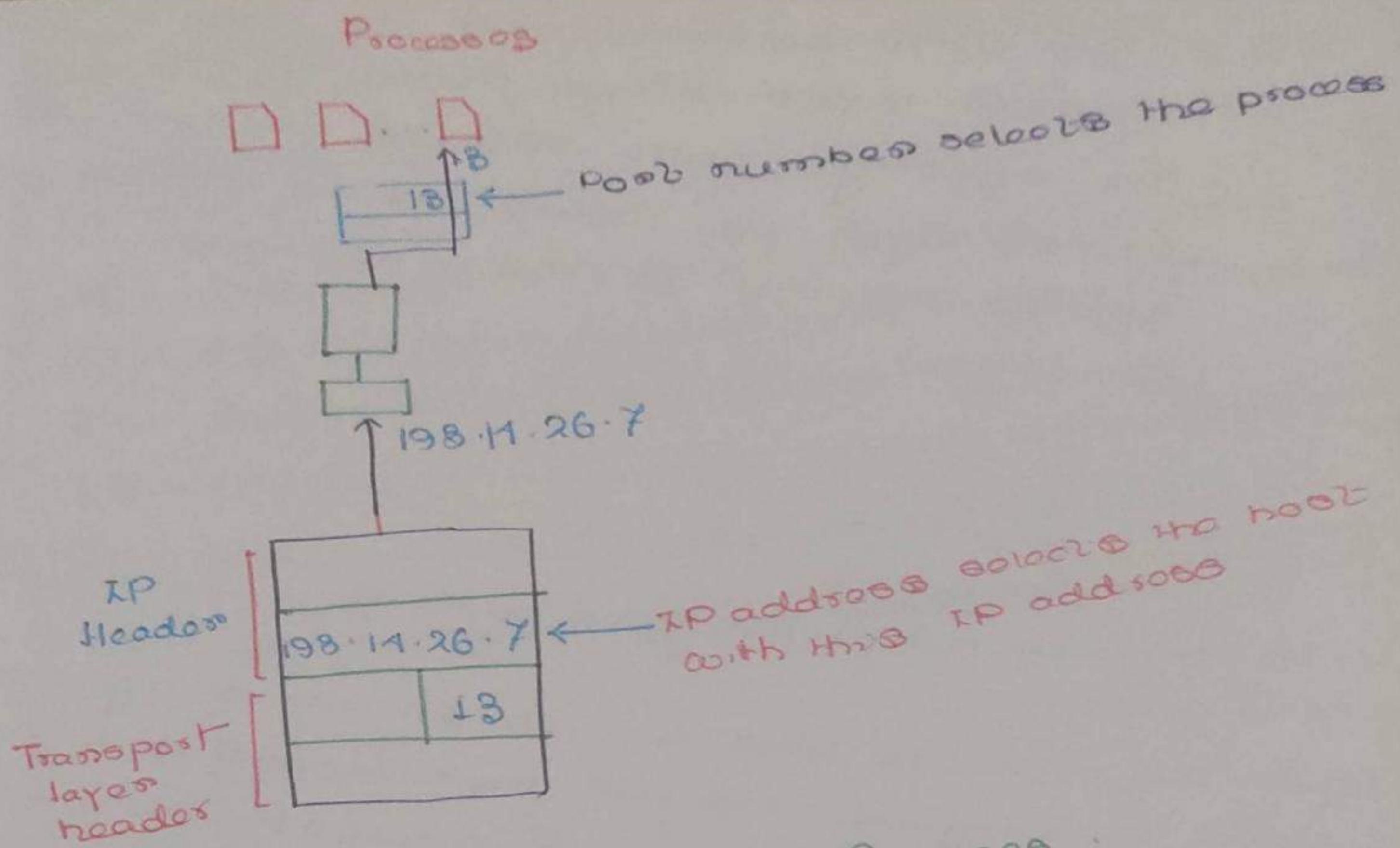
Process to Process: Transport layer (Port no.)

Each process is identified by a unique port no.

Day home servers



DP = Destination Port No.
SP = Source Port No.



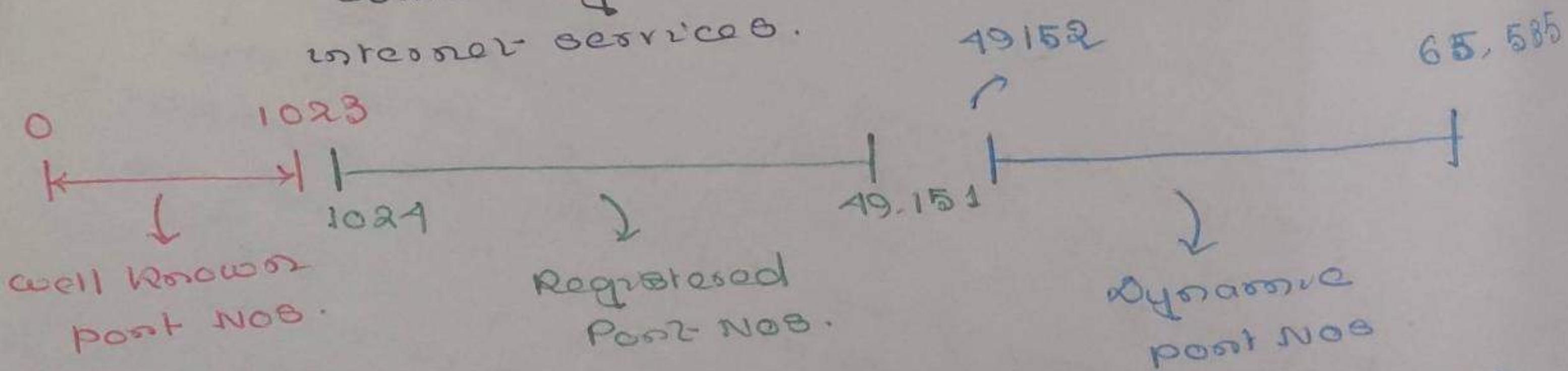
Multiplexing and Demultiplexing vs done at the transport layer. As many processes are running at one time in the application layer. But only one transport layer is present. So multiplexing vs done and port addresses are embedded to the next layer that is transferred to the network layer and is at the receiver side after receiving the network layer datagram the network layer headers will be removed and

The packet will be transferred to the transport layer. After demultiplexing the message with specific port address will be delivered to the specific process at the receiver device.

Port Numbers:-

- (1) In computer networking, a port is a communication end point.
- (2) At the software level, within an operating system a port is a logical construct that identifies a specific process or a type of network service.
- (3) A port is identified for each transport protocol and address combination by a 16-bit unsigned number, known as the port number.
- (4) The most common transport protocols that use port numbers are the TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Port numbers :- This includes the registration of commonly used port numbers for well-known interior services.



The port numbers are divided into three ranges

- ① Well Known
- ② Registered
- ③ Dynamic or Private ports.

2. Registered Port Numbers

The registered ports are those from 1024 through 49,151.

- * IANA (Internet Assigned Numbering Authority) maintains the official list of well-known and registered ranges.
- * IANA is responsible for the global coordination of the DNS root, IP addressing, and other internet protocol resources.
- * This includes the registration of commonly used port numbers for well-known internet services.

3. Dynamic Port Numbers :- (Private port numbers)

Range from 49,152 to 65,535 (i.e. 2¹⁶).

- * Ranges from 49,152 to 65,535 (i.e. 2¹⁶).
- * Assigned by the operating system dynamically (suppose we are browsing www.google.com from our pc/laptop then this will assign a dynamic port no to this process. As the destination port nos are very important so well-known port nos are assigned to the destinations)

*

port numbers in URLs

- * Port numbers are sometimes seen in web or other uniform resource locators (URLs).
- * By default, HTTP uses port 80 and HTTPS uses port 443.
- * URL - `http://www.example.com:8080/path/` specifies the web browser to connect to port 8080 of the HTTP server.

In application layer many processes are running simultaneously. For process-to-process delivery of data we have seen port numbers are very important. When the application layer data is passed to transport layer, the transport layer headers are appended to the data. It may be TCP (Transmission control Protocol) and UDP (User Datagram Protocol) headers depending on the information content.

Some information communication can allow some delay but cannot compromise on the reliability (i.e. data losses) and some information communication can allow some losses on the other hand cannot allow any delay.

Data link layer - communication is done using MAC addresses i.e. hardware address.

Network layer / internet layer - communication is done using IP addresses or internet protocol addresses. These are often named as software addresses.

Transport layer— communication is done using port addresses of both the source process and the destination process.

The transport layer moves

Application layer— data between applications or devices in the network

Application layer → Is the direct interface between users and data are generated & received at this layer

Two important protocols

- TCP (Reliable)

- ~~UDP~~

- No loss but delay

- e.g. → Email

- some delay can be allowed by no loss in information is not allowed

- Retransmission is not possible.

(1) HTTP (website/webbrowsers)

(2) FTP

(3) SMTP

(4) Telnet (Remote login)

- UDP (unreliable)

- No delay but loss

- Real time traffic

- Video conferencing, conferencing, live call.

- Delay may introduce chaos in the communication and retransmission is also not possible.

(1) DHCP

(Dynamic Host configuration protocol)

(2) DNS

(3) SNMP

(4) TFTP

(5) VoIP

uDP (User Datagram Protocol):-

- Simple protocol that provides the basic transport layer function.
- used by applications that can tolerate tolerate small loss of data (as no retransmission is possible)
- used by applications that cannot tolerate delay

used by:-

① DNS

② VoIP

③ SMTP SNMP (Simple Network Management Protocol)

④ DHCP

(5) TFTP (Trivial File Transfer Protocol)

(6) Online games.

→ no connection establishment between source & destination

* connectionless and unreliable.

* Prior communications (as handshaking) are not required in order to setup communication channels on data paths.

* UDP-based servers applications are assigned well-known or registered port numbers.

* UDP client process randomly selects port numbers from range of dynamic port numbers (these are operating system assigned port numbers) as the source port

* UDP is suitable for purposes where error checking and correction are either not necessary or are performed in the applications uDP avoids the overhead of such processing in the protocol stack.

* NO error correction.

~~UDP~~ ~~UICP~~ Time-sensitive applications often use

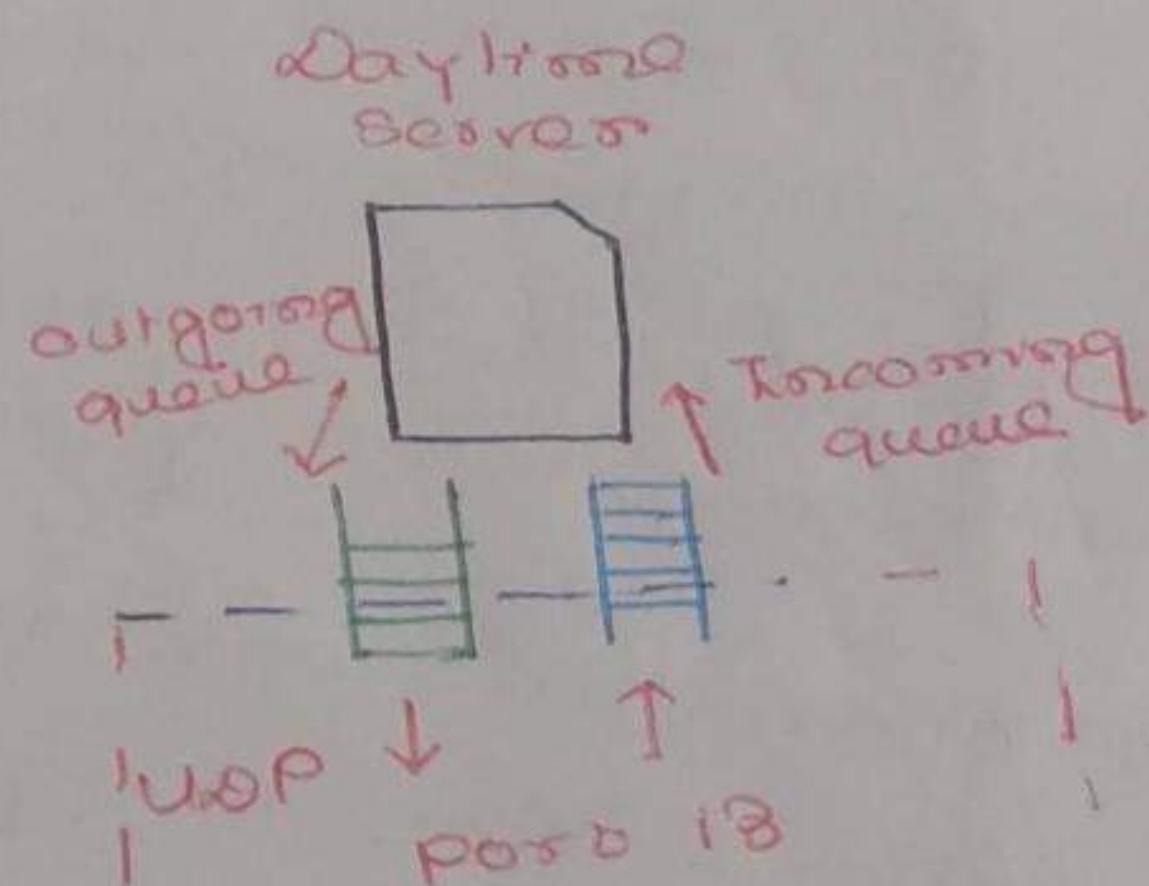
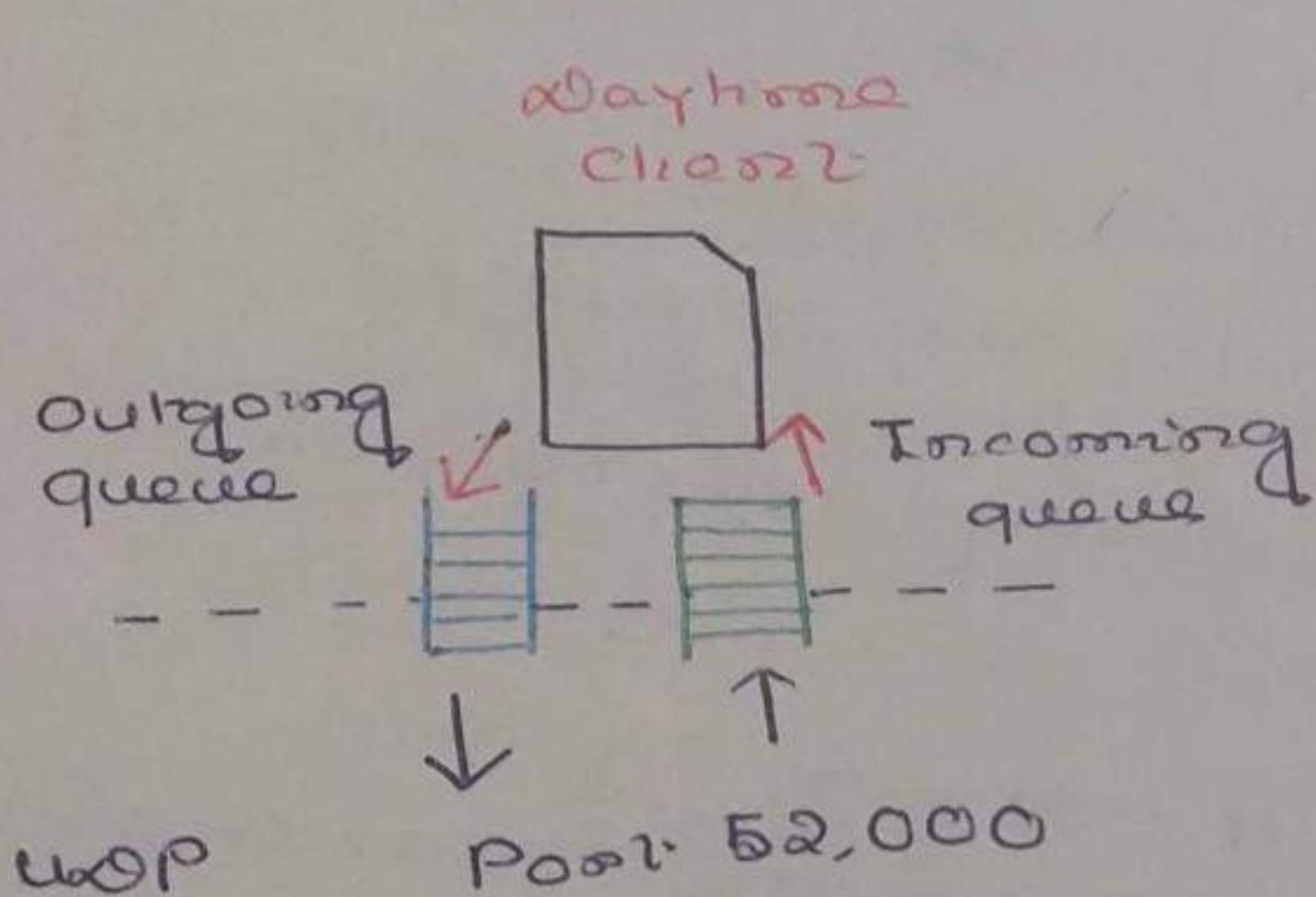
UDP because dropping packets is preferable than to waiting for packets due to retransmission which may not be an option in a real-time traffic on system.

* No Flow control mechanism.

The UDP ^{headers} ~~packets~~ are very simple and have only four fields. These UDP headers are kept simple because UDPs are used for real-time communication so when a source receives an UDP packet it should not take more time to process it.

* Encapsulation and Decapsulation is done by the UDP protocol.

* Queuing is done the UDP.

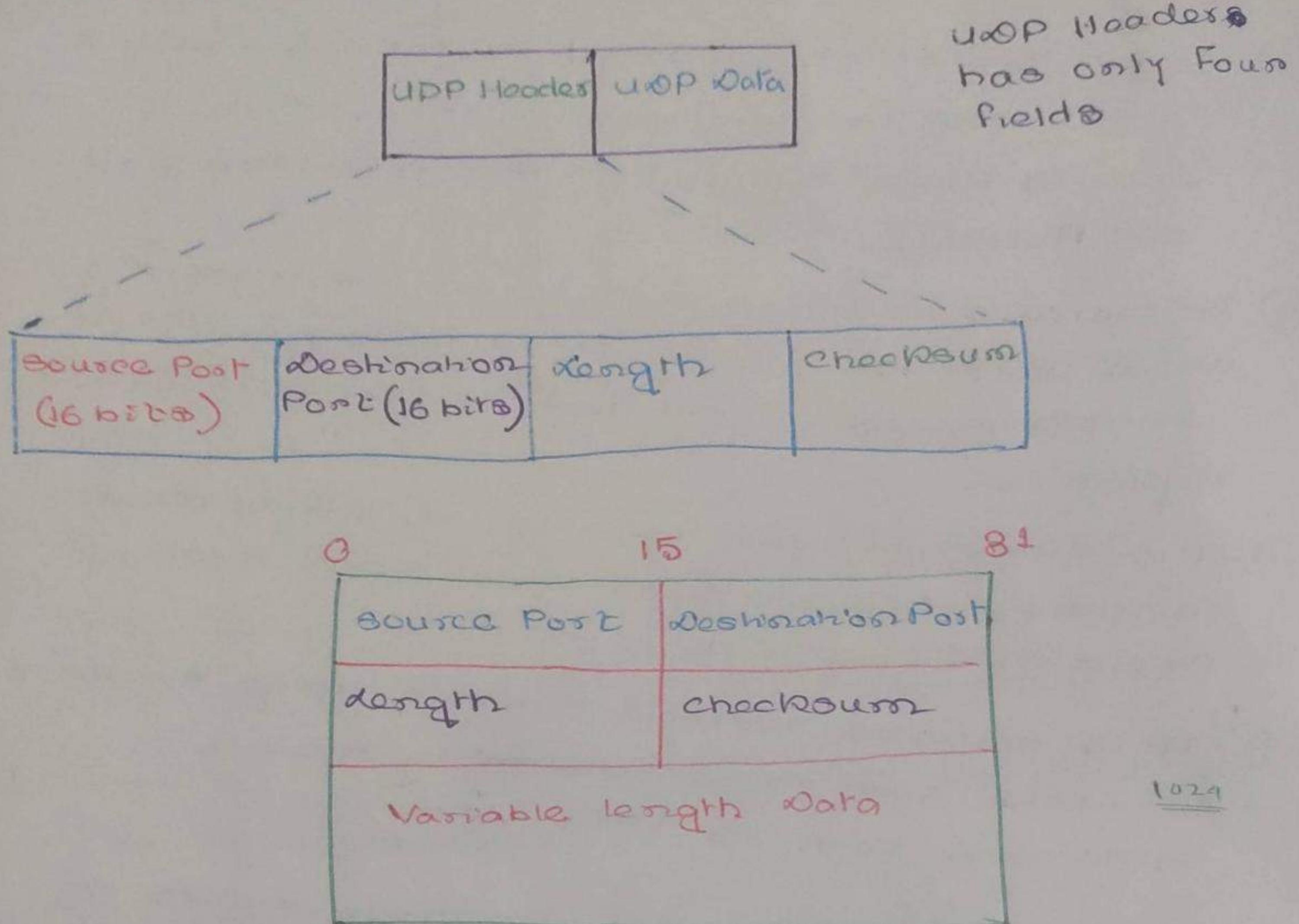


In application layer many processes are running simultaneously. If the client has two queues the server also has to maintain two queues. The UDP dequeues messages one after another and adds UDP header and passes it to the next layer i.e. network layer to add IP header. When the process are terminated at the application layer, the queues are also discarded.

USES OF UDP:-

- ① It is a transaction-oriented, suitable for simple request-response protocols such as DNS (Domain Name System) or the NTP (Network Time Protocol).
- ② It provides datagrams, suitable for modeling other protocols such as IP tunneling or remote procedure call and the Network File system.
- ③ It is simple, suitable for bootstrapping or other purposes without a full protocol stack, such as the DHCP and TFTP.
- ④ It is stateless, suitable for very large numbers of clients, such as in streaming media applications such as IPTV. (because of simplified header).
- (5) The lack of retransmission delay makes it suitable for real-time applications such as VoIP, online games, and many real-time streaming applications.
- (6) UDP is a suitable transport protocol for multicasting. Multicasting capability is embedded in the UDP software but not in the TCP software.
- (7) UDP is used for some route updating protocols as routing information protocol (RIP).

UDP Header Format :-



All the four field are of 16 bits length.

Source port Number :-

- This is the port number used by the process running on the source host. usually this port number is assigned by the operating system.
It is a 16-bit long, which means that the port number can range from 0 to $(2^{16}) - 1$, i.e. 65,535.
- If the source host is the client (a client sending a request), the port number is most cases is an ephemeral port number i.e. random port numbers greater than 1024 (well known and registered) requested by the process and chosen by the UDP software running on the source host.

- If the source host is the server (a client sending a response), the port number in most cases is a well-known port number.

Destination Port number:-

- This is the port number used by the process running on the destination host.
- It is also 16 bits long. If the destination host is the server (a client sending a request), the port number, in most cases, is a well-known port number.
- If the destination host is the client (a server sending a request response), the port number in most cases, is a ephemeral (i.e. random) port number.
- In this case, the server copies the ephemeral port number it has received in the request packet.

Length Field:-

- This is a 16-bit field that defines the total length of the user datagram, header plus data. The 16 bits can define a total length of $0\text{ to } (2^{16}-1)$ i.e. 65,535 bytes.
- However, the total length of the user datagram need to be much less because a UDP user datagram is again stored in an IP datagram with a total length of 65,535 bytes.
- $\text{UDP length} = \text{IP length} - \text{IP header's length}$

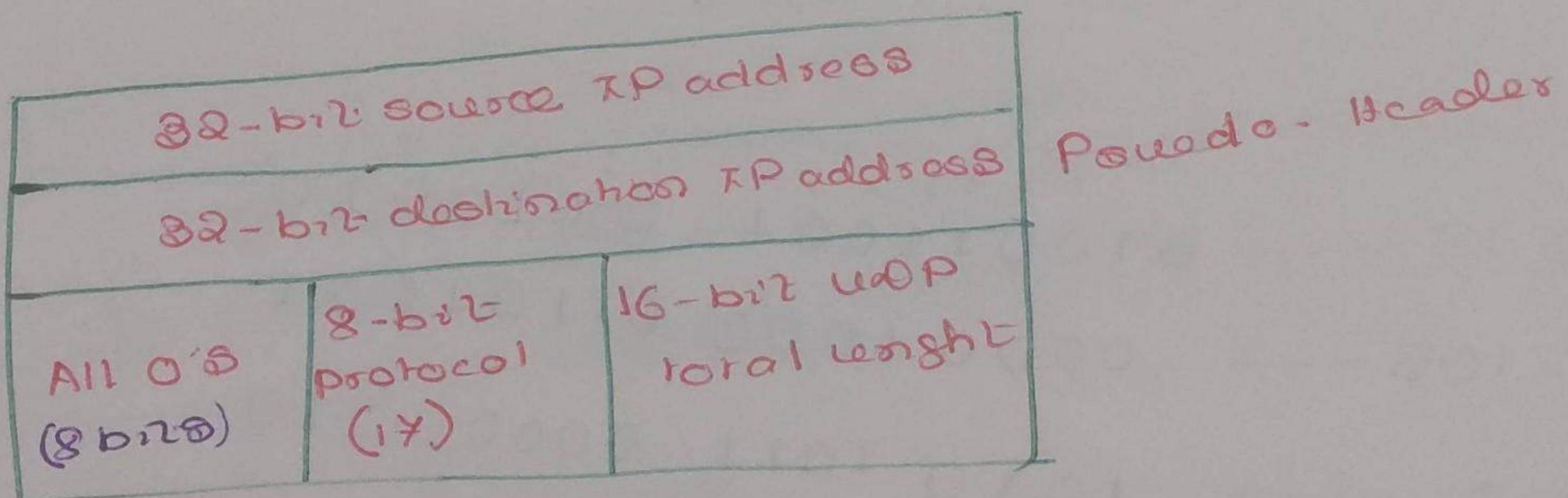
UDP checksum

Pseudo-header in UDP:-

- The UDP checksum calculation is different from one for IP and ICMP.
 - In UDP, the checksum includes three sections:
 - A Pseudo-header
 - The UDP header and
 - The data (coming from the application layer).
 - The pseudo-header is the part of the header of the IP packet in which the user datagram is to be encapsulated with some fields filled with 0's (zeroes).
 - If the checksum does not include the pseudo-header, a user datagram may be delivered with out errors.
 - However, if the IP header is corrupted, it may be delivered to the wrong destination.
- The data generated by the top-most layer that is the application layer pass to the transport layer where the UDP header is encapsulated with the data. Now in the network layer along with the IP header a header field containing 0's is

added at the IPV4 field filled with 0's which is called as Pseudo-header.

- The protocol field is added to ensure that the packet belongs to UDP and not to other transport layer protocols.
- The value of the protocol field for UDP is 17. If the value is changed during transmission, the checksum calculation at the receiver will detect it and UDP drops the packet and will not deliver to the wrong destination.



Source Port Address (16 bits)	Destination Port Address (16 bits)
UDP total length (16 bits)	Checksum 16 bits
Variable length data	

UDP Header

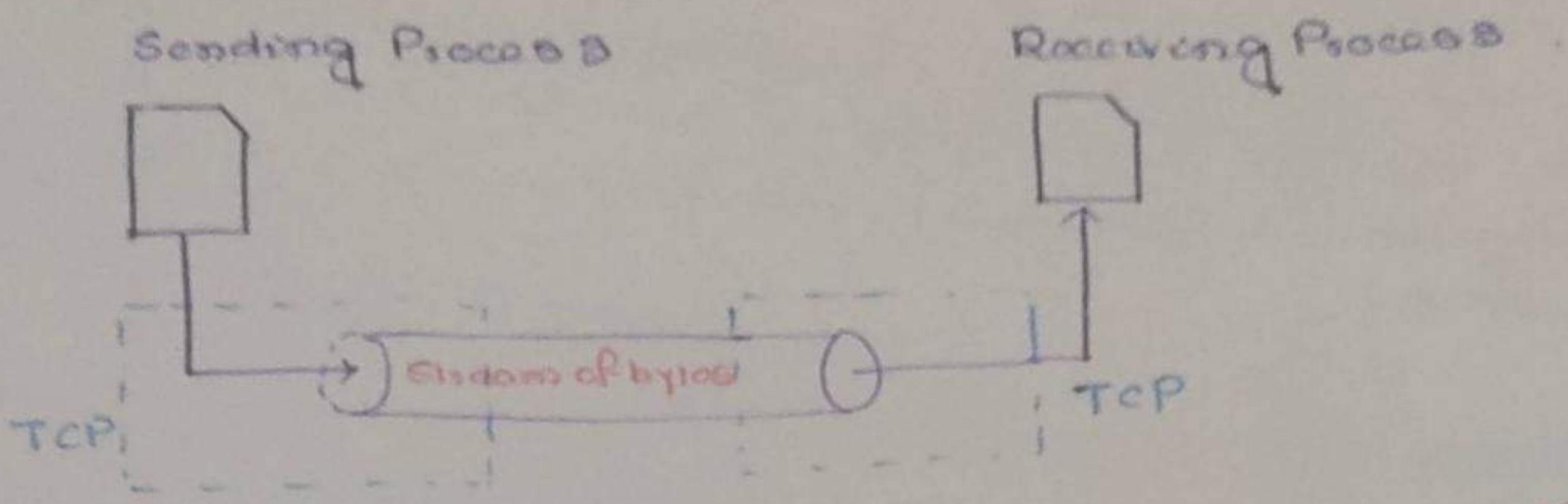
TCP (Transmission control protocol) :-

- TCP is the widely used Transport layer protocol.
- It creates a virtual connection between two TCPs to send data.
- In addition, TCP uses flow and error control mechanisms at the transport level.
- Used by applications that can tolerate delay but cannot tolerate loss.
- Used by proto applications such as:
 - ① HTTP
 - ② FTP
 - ③ Telnet
 - ④ SMTP
 - ⑤ World wide web (www)

Features of TCP

- TCP is a connection oriented protocol. Connection is established using three way handshaking before starting the communication.
- Reliable delivery (sender will know receiver has received the data or retransmission will be done)
- Acknowledgment oriented.
- Retransmission.
- Flow control (Speed control mechanism)
- Error control
- Congestion control
- Segmentation and Reassembly
- Full Duplex Support.

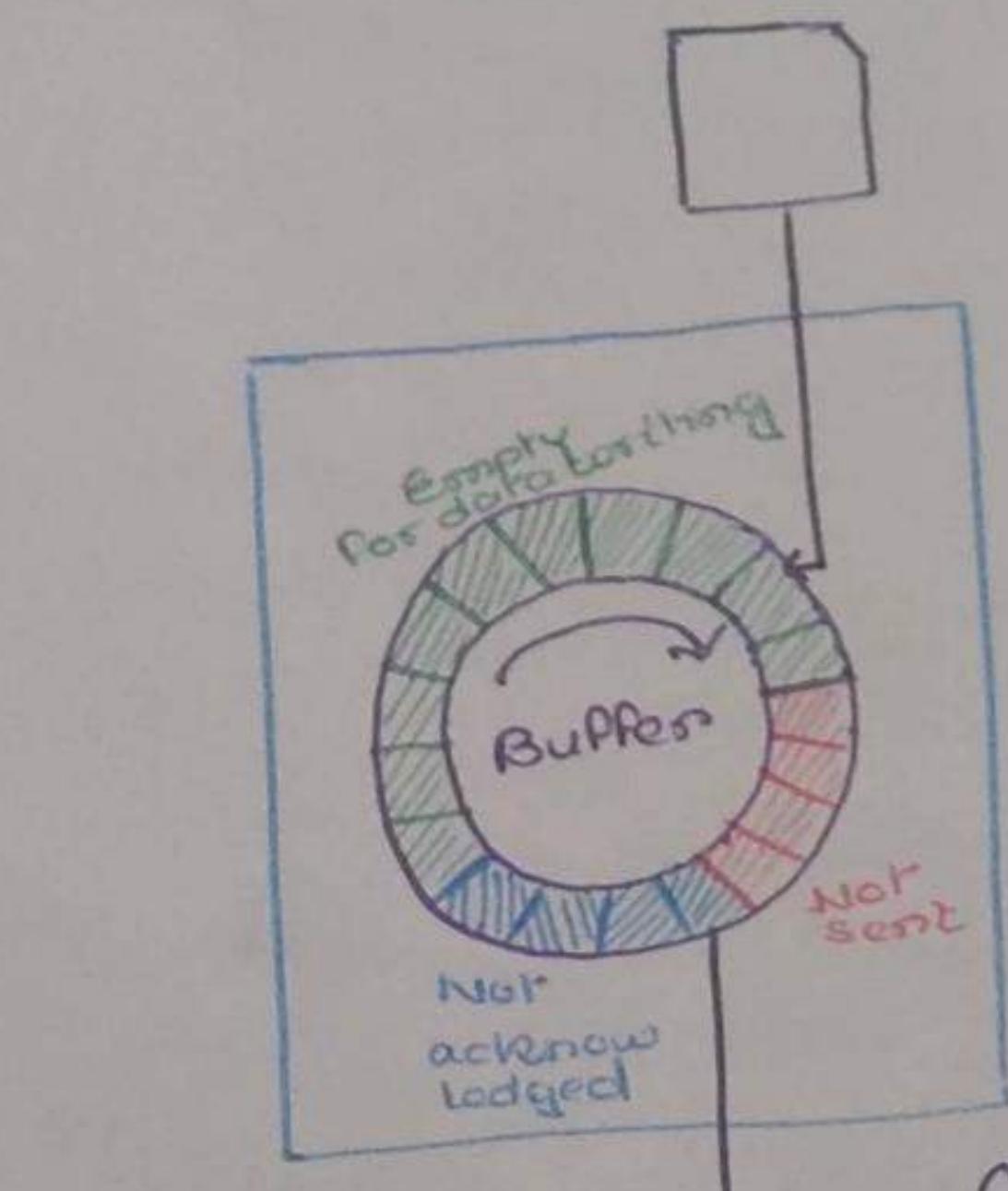
TCP Stream delivery:-



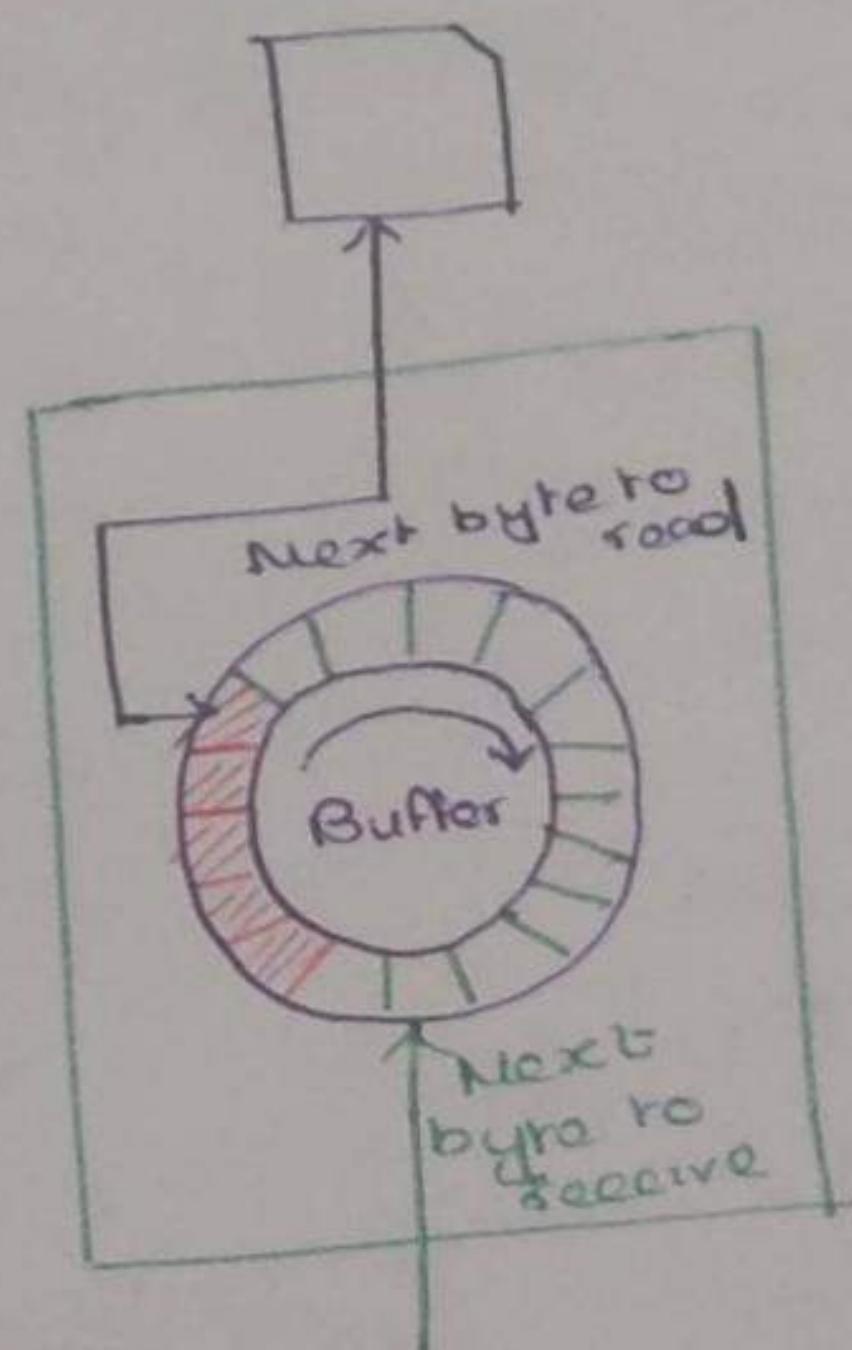
This sending and receiving process are running in two different system (e.g. computer/laptop/cellphones). This imaginary tube will deliver the data in form of stream of bytes.

TCP sending and Receiving Buffer:-

Sending Process



Receiving Process



- Red color indicated data bytes which are not sent.

- Blue cells indicate data sent by not acknowledged

- Green indicated empty buffer where data will be stored

"After acknowledgement"

received the data, chambers will be recycled.

TCP segments:-

Each segment can be of different lengths.
Each segment carries hundred or thousand of bytes. The TCP adds TCP headers to each of the segment for control and error detection activities.

Application layer generates data



This data is passed to the transport layer

The transport layer add TCP headers and make segments consists of data stream bytes of data bytes. Transport layer user datagrams are called segment



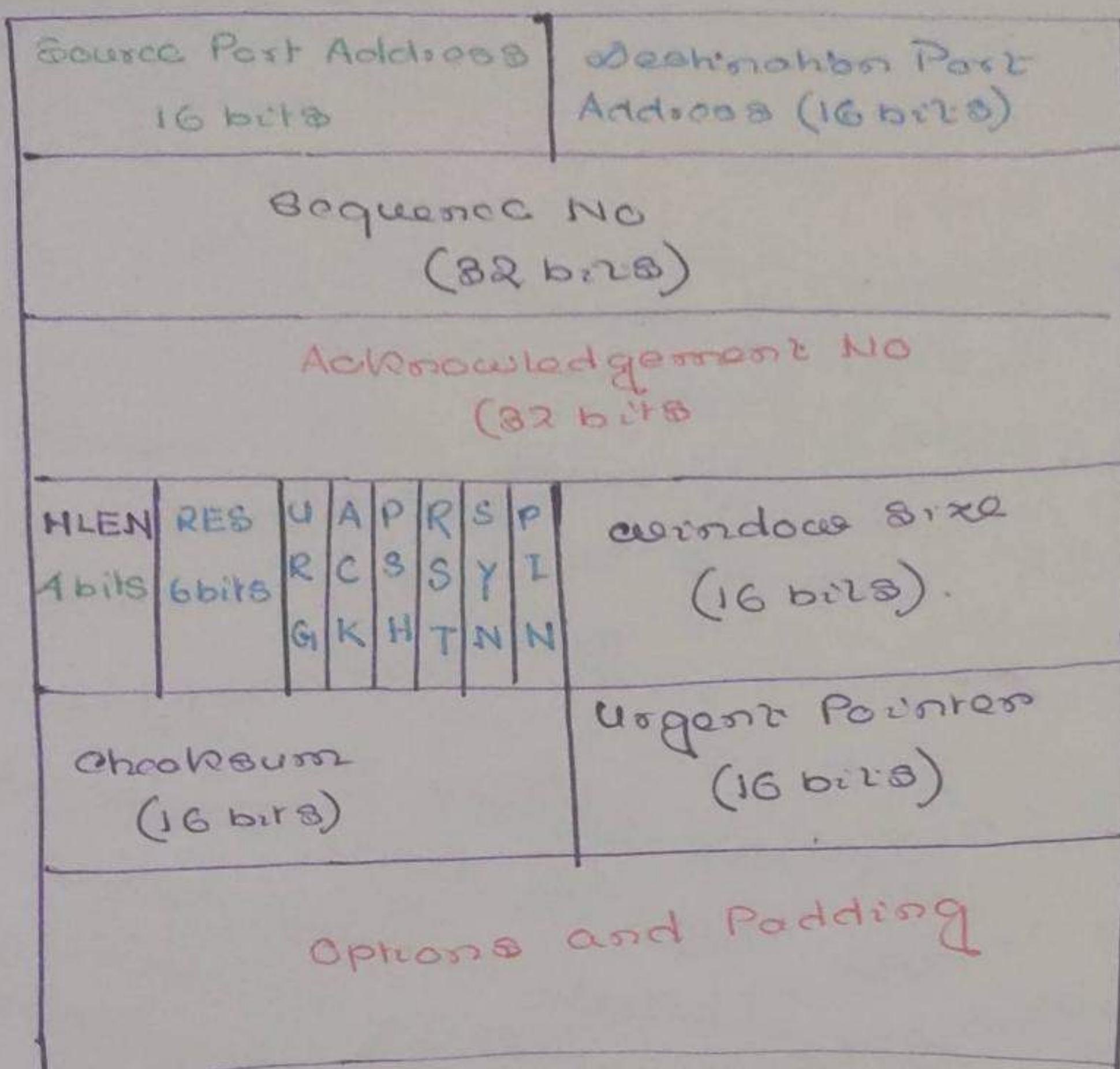
The segments will be passed to the network layer. And in this layer IP headers will be embedded to the segments. These network layer datagrams are called IP packets. If TCP headers are added then it is called segment. In UDP headers are also added.

The IP packets are then sent to the data link layer for transmission. In this layer the communication work can be done on wireless. The data link layer will add their header to the IP packets received from the network layer, and will make a frame.



This will be pass to the physical layer and this layer will convert the received frames from the data link layer to electromagnetic signals on optical signals. The physical layer protocol data units are called bits.

TCP Header Format :-



if options are added than 60 bytes

(Minimum Header)

The TCP header length is 20 bytes. (Minimum length)
 The TCP header plus options and padding length can go upto 60 bytes, i.e. The options and padding length can maximum go upto $(60 - 20) = 40$ bytes.

We have seen that the UDP has only 1-fields, whereas TCP/IP has more no. of fields.
 As TCP provides a reliable and acknowledgement oriented communication with error control and flow control mechanism.

Source Port Number:-

(1) It defines the port number of the application program in the host device that is sending the segment. We have seen in a client host many processes are running simultaneously. The process which is sending/receiving the data, this port number is associated with the process.

(2) This serves the same purpose as the source port address in the UDP header.

Destination Port address:-

- (1) It defines the port number of the application program in the host that is receiving the segment (well known port numbers).
- (2) This serves the same purpose as the destination port address in the UDP header.

Sequence Number:-

This is a 32-bit field that defines the number assigned to the first byte of data contained in the segment. This sequence number helps us to know about missing packets, lost packets, out of order and delayed packets.

Has a dual role:-

- If the SYN flag is set to 1, then this is the initial sequence number. The sequence number of the actual first data byte and the acknowledged number is the corresponding ACK are then this sequence number plus 1.
- Suppose the sequence number of the first data byte is 1001 then the acknowledgment (ACK) number sent by the receiver is 1002 i.e. the receiver is expecting the second data byte.
- If the SYN flag is 0, then this is the accumulated sequence no. of the first data bytes of this segment for the current session.

Acknowledgment number:-

- (1) Thus is a 32 bit field.
- (2) It defines the byte number that the receiver of the segment is expecting to receive from the other party.
- (3) If the receiver of the segment has successfully received byte numbers x from the other party it defines $(x+1)$ as the acknowledgement number. Acknowledgments and data can be piggybacked together.

hlen (Header length):-

- It indicates the number 4-byte words in the TCP header.
- The length of headers can be 20 bytes to 60 bytes i.e. $(60 - 20 = 40)$ bytes vs options & padding
- Therefore, the value of this field can be between 20 bytes i.e. $(5 \times 4 = 20)$ to 60 bytes i.e. $(15 \times 4 = 60)$. As the hlen field contains 4-byte words.

RES (Reserved field)

- It is a 6-bit field.
- It is reserved for future use and usually filled with 0's.

(e) Flag bits in TCP header:-

U	A	P	P	S	F
R	C	S	S	Y	I
G	K	H	T	N	N

(i) Fields
Flag bits are consists of 6 different control bits
on Flags each of the 6 flags are of 1 bit.
One or more of these bits can be set at a time.

(2) URG (1 bit):- when this is set v.e. L the urgent pointers field hold its significance.

S ACK (1 bit):- indicates that the acknowledgement field is significant.

T PUSH (1 bit):- push function. ACK' 20 push the buffered data to the receiving application.

RST (1 bit):- Reset the connection.

SYN (1 bit):- synchronise sequence numbers.

FIN (1 bit):- last packet from sender.

window size :-

- This field defines the size of the window. i.e. by 10s, that the other party must maintain.
- Suppose the receiver's window is of 20 bytes. Receiver can handle 20 bytes at a time. But if the sender without knowing the receiver's window sends 50 bytes then it can only receive 20 bytes and other bytes will be discarded. So it is very important for the receiver to inform about its window size.

This field defines the size of the window.

- The length of this field is 16 bits, which means that the maximum size of the window is

$$(2^{16}-1) = 65,535 \text{ bytes.}$$

- This value is normally referred to as the receiving window (window) and is determined by the receiver.

- The sender must obey the dictation of the receiver in this case.

checksum :-

- The calculation of the checksum for TCP follows the same procedure as the one described for UDP.
- However, the inclusion of the checksum in the UDP datagram is optional (i.e. if checksum is not added by the UDP layer to calculate), whereas the inclusion of the checksum for TCP is mandatory.
- The same pseudo-header, serving the same purpose, is added to the segment for the TCP pseudo-header. The value of the protocol field is 6. (For UDP or is 17)

Urgent Pointer :-

- ① This 16-bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data.
- We have seen the real-time traffic on urgent data is normally sent by the UDP transport protocol. But in some case we want a data to be sent urgently and also maintains its reliability. Then this is used in TCP.
- This is defined as the number that must be added to the sequence number to obtain the number of the last urgent byte in the data section of the segment.

Options:-

- This field can be upto a maximum of 40 bytes. These can be upto 40 bytes of optional information in the TCP header.
- The length of this field is determined by the Data offset field. Options have up to three fields:-
 - Options - Kind (1 byte)
 - Options - length (1 byte).
 - Options - data (variable).

Padding:-

The padding is composed of zeros. The TCP header padding is used to ensure that the TCP header ends, and data begins, on a 32-bit boundary.

TCP connection:-

1. connection-oriented
2. virtual path (seq + acknowledgement).
3. Acknowledgment process
4. Retransmission of lost damaged frames
5. TCP connection - virtual or physical
6. IP - connectionless
7. Full-duplex mode
8. Approval from other party

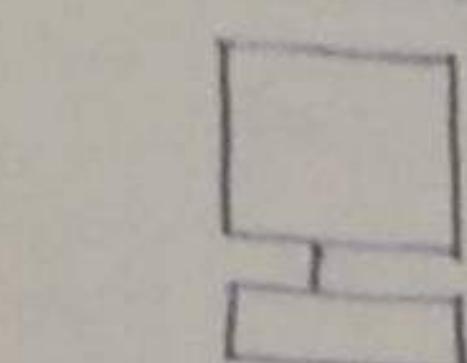
Three phases of TCP connection

1. Connection Establishment
2. Data transfer
3. Connection Termination

TCP connection establishment:-

Three-way-handshaking mechanism:-

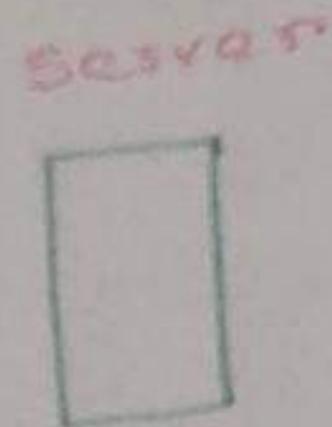
- Client



SYN

SYN+ACK

ACK



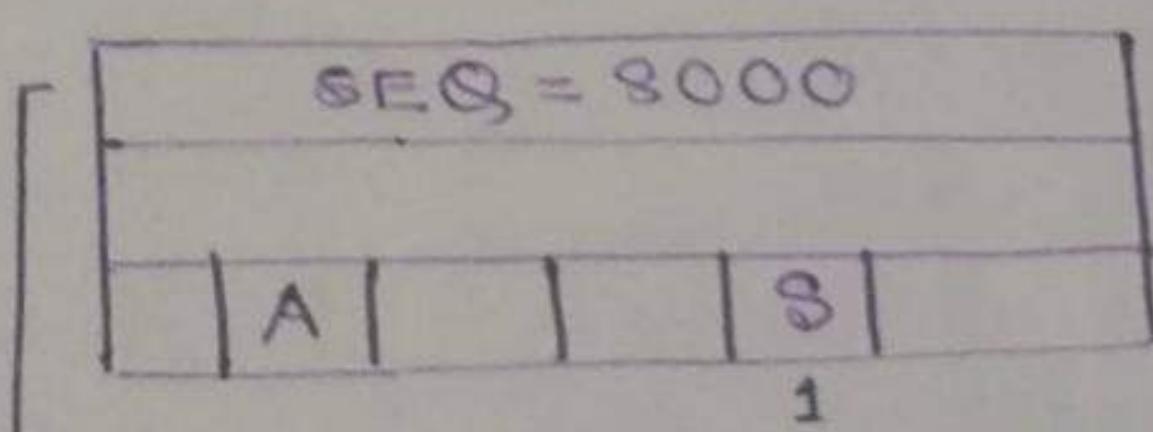
Time

Time

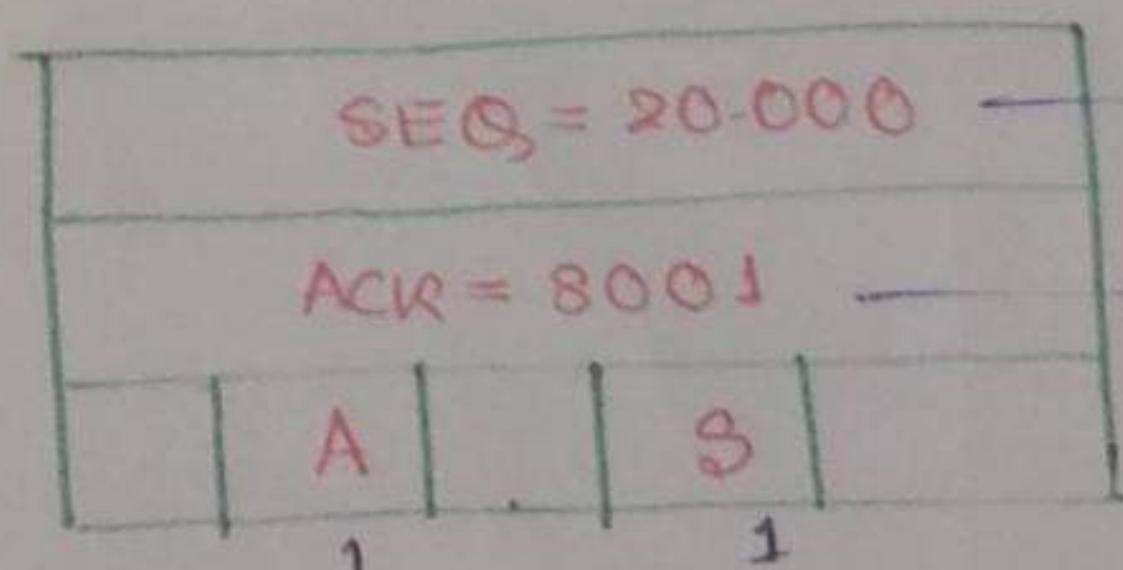
Three segments are exchanged three way it is called Three-way Handshaking

- client will initiate the connection to also initiate the connection. But in this case, the server has with passive open. Means the server has to inform that he is ready to accept messages.

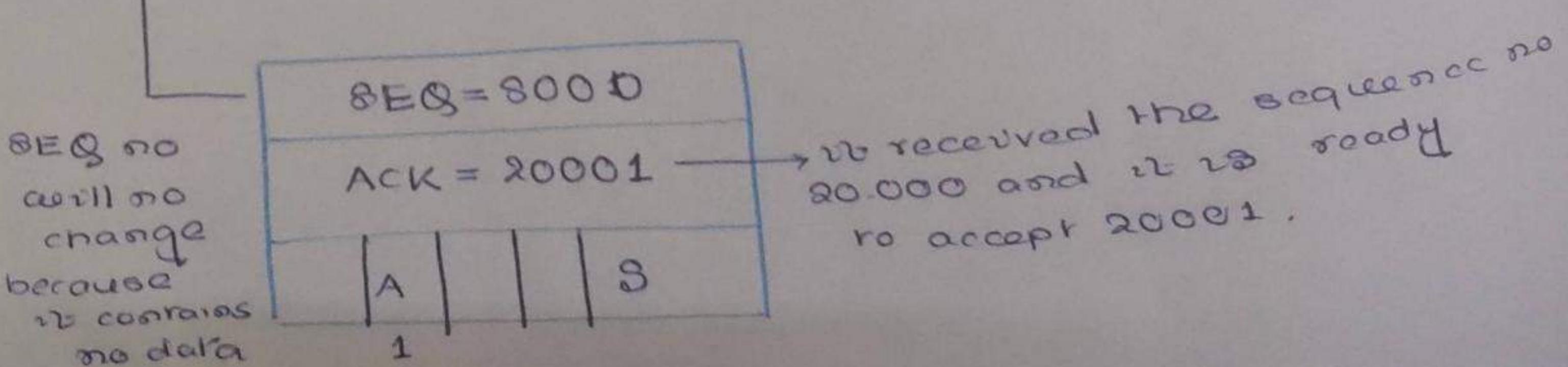
SYN (from the client) Flag is set



SYN+ACK (from the server)



ACK (from the client)



SEQ no will not change because it contains no data

→ received the sequence no 20000 and it is ready to accept 20001.

TCP Data Transfer:-

2. Data Transfer

Bi-directional Data Transfer

(From client data and server sends ACK)

- Segment can carry both data + acknowledgement means the acknowledgement is piggybacked with data

Push and Urg Flags

- receiving TCP should handover the ~~rec~~ segment to the receiving application urgently

immediately.

before the buffer

overflows to be filled up.

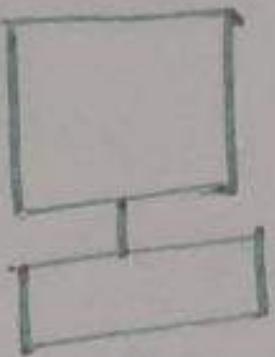
or should not wait

for the buffer to be filled

Data bytes which
are urgent message
as suppose (control)

means about operation
this message
should be executed
urgently.

client



SEQ = 8001
ACK = 15001
A P
Data bytes (8001 - 9000)

server



Assume that the
three-way
handshaking is
done and
now only data
transmission is
going on

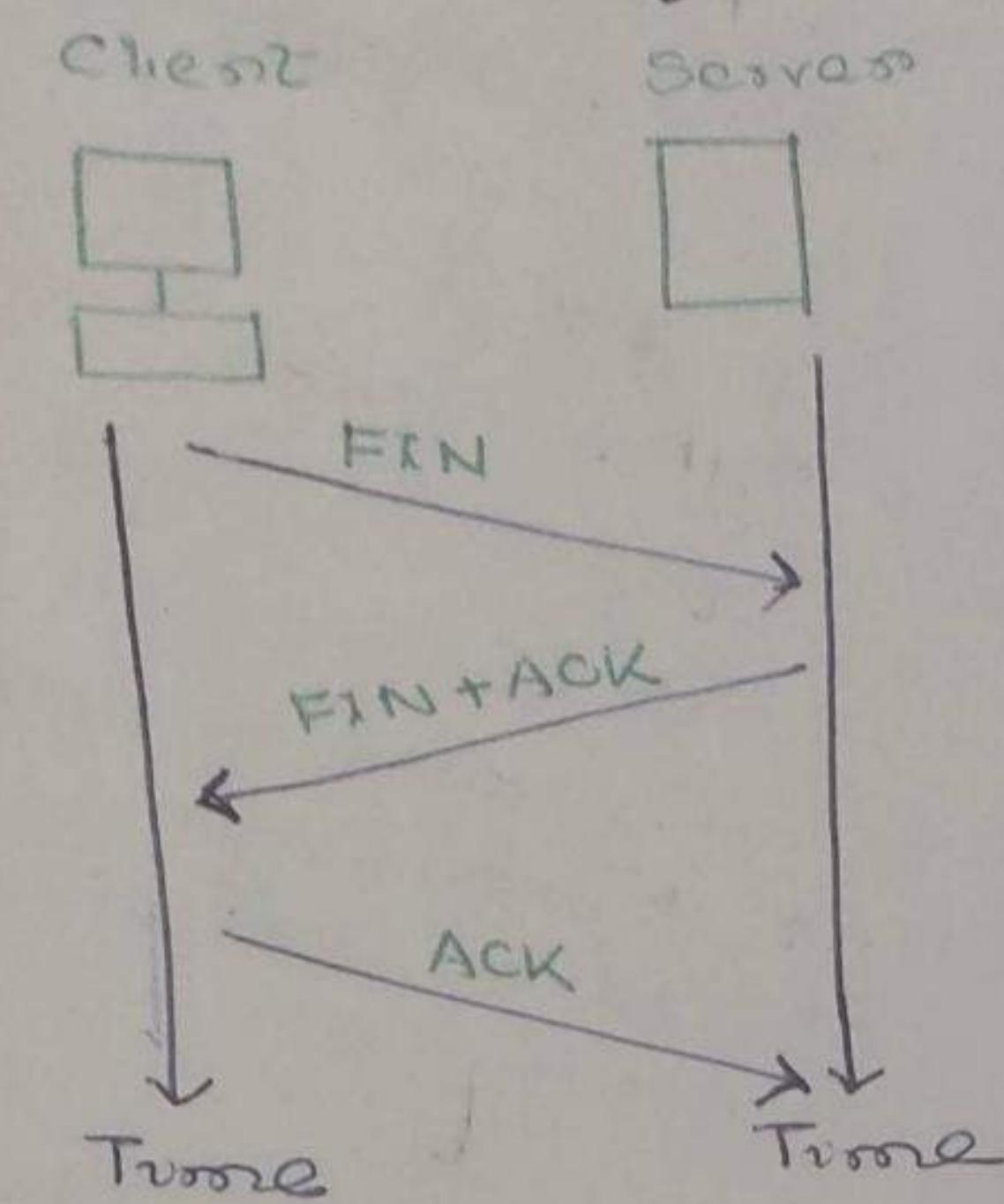
SEQ = 9001
ACK = 15001
A I P I I
Data bytes (9001 - 10000)

SEQ = 15001
ACK = 10001
A I
Data bytes 15001 - 17000

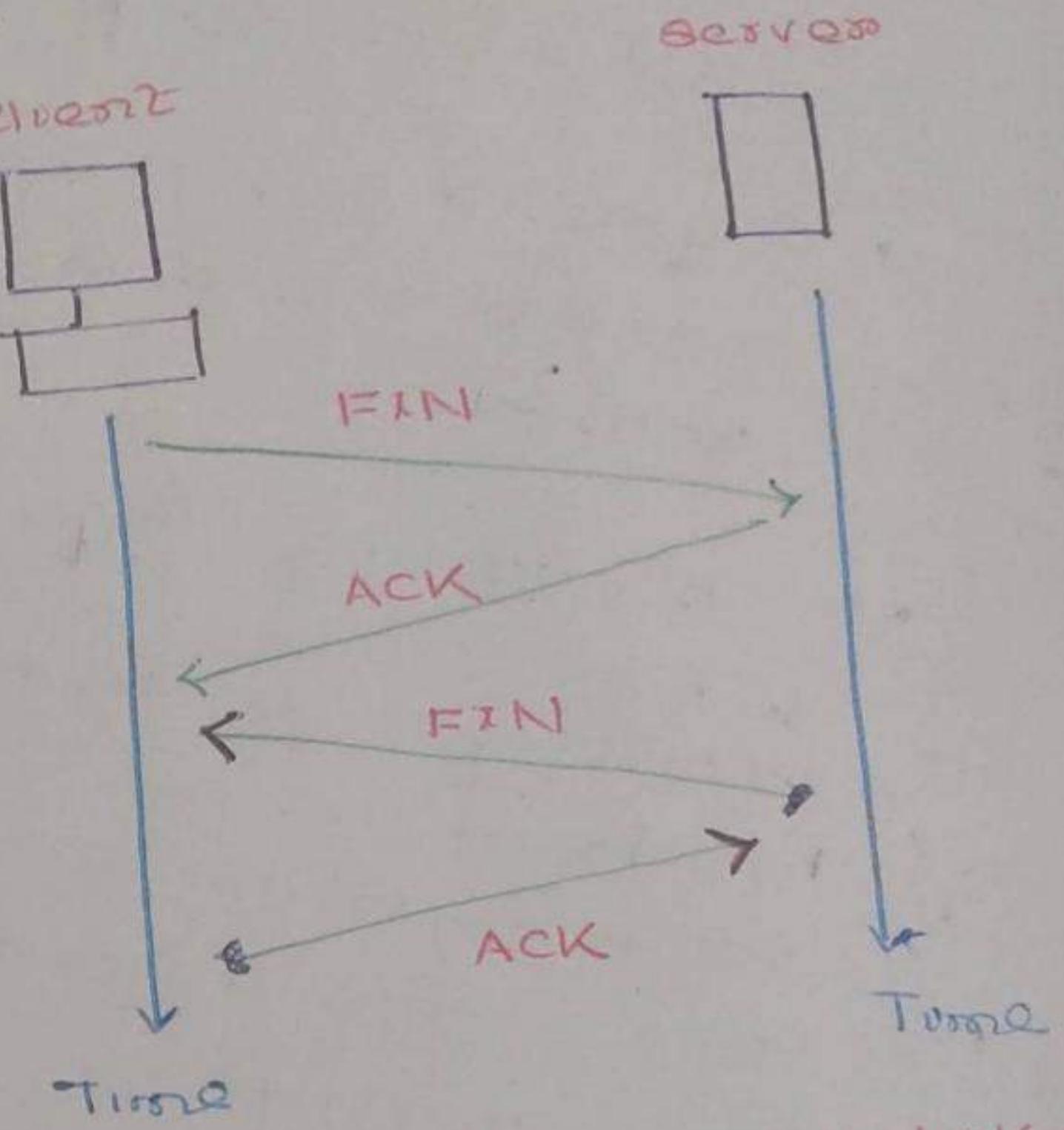
SEQ = 10000
ACK = 7000
A I I I

TCP connection Termination:-

- Usually connection termination is initiated by the client.
- Two options for connection termination.
 - Three way handshaking
 - Four way handshaking and a half-close option.



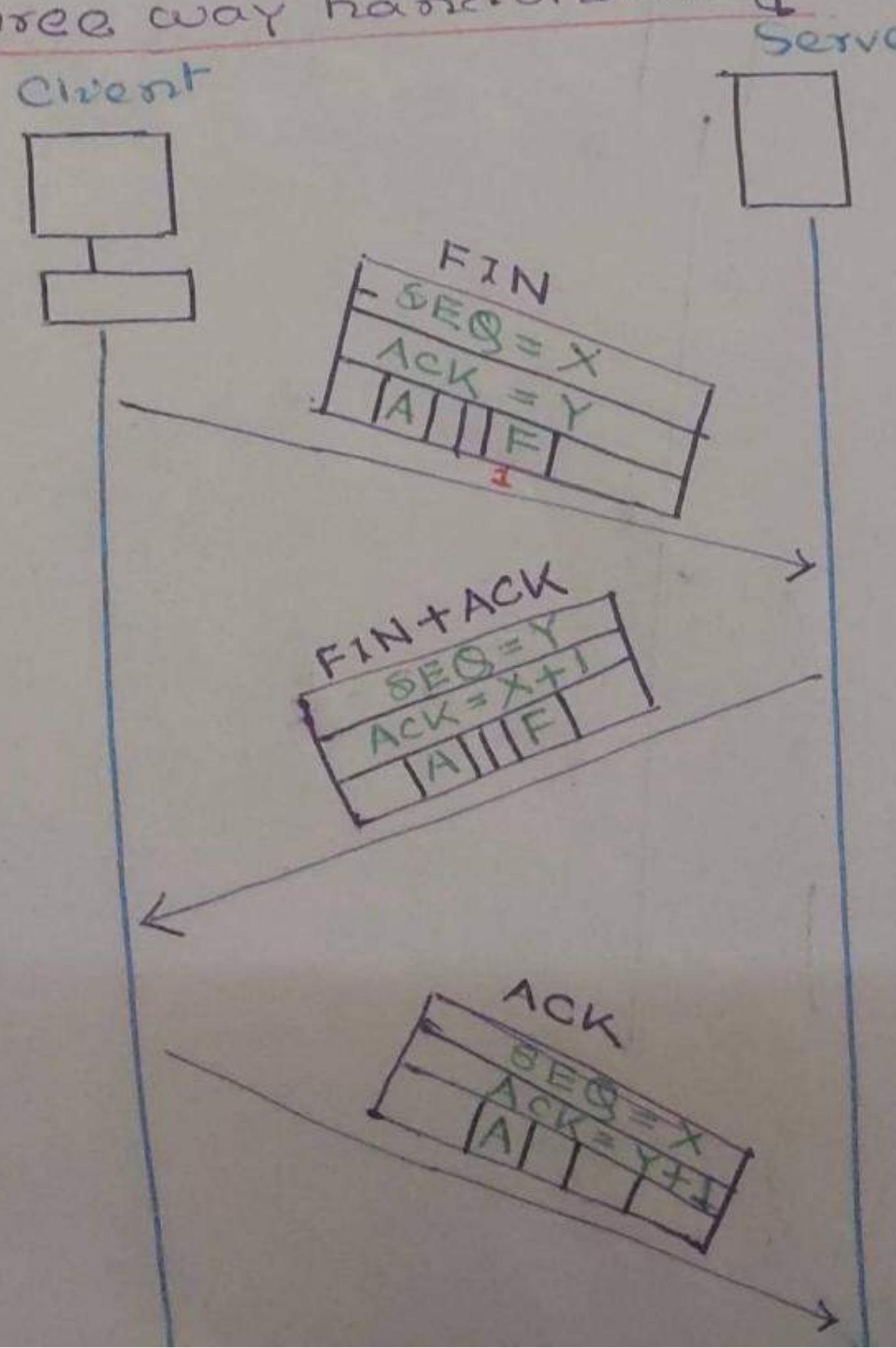
Three-way handshaking



Four-way handshaking

Both client and server can close the connection.

Three way handshaking:-



when server is initiating finish (FIN) then the server is no more allowed to send data. This FIN segment can be embedded with the last data segment. But in this time the server can send both data and acknowledgement till the server is not sending any FIN message.

Module 4

Transport Layer



Dr. Sunandita Debnath, IIIT Vadodara

TCP

Features of TCP

□ Connection oriented

□ Reliable delivery ✓

□ Acknowledgement oriented

□ Retransmission

□ Flow control ✓

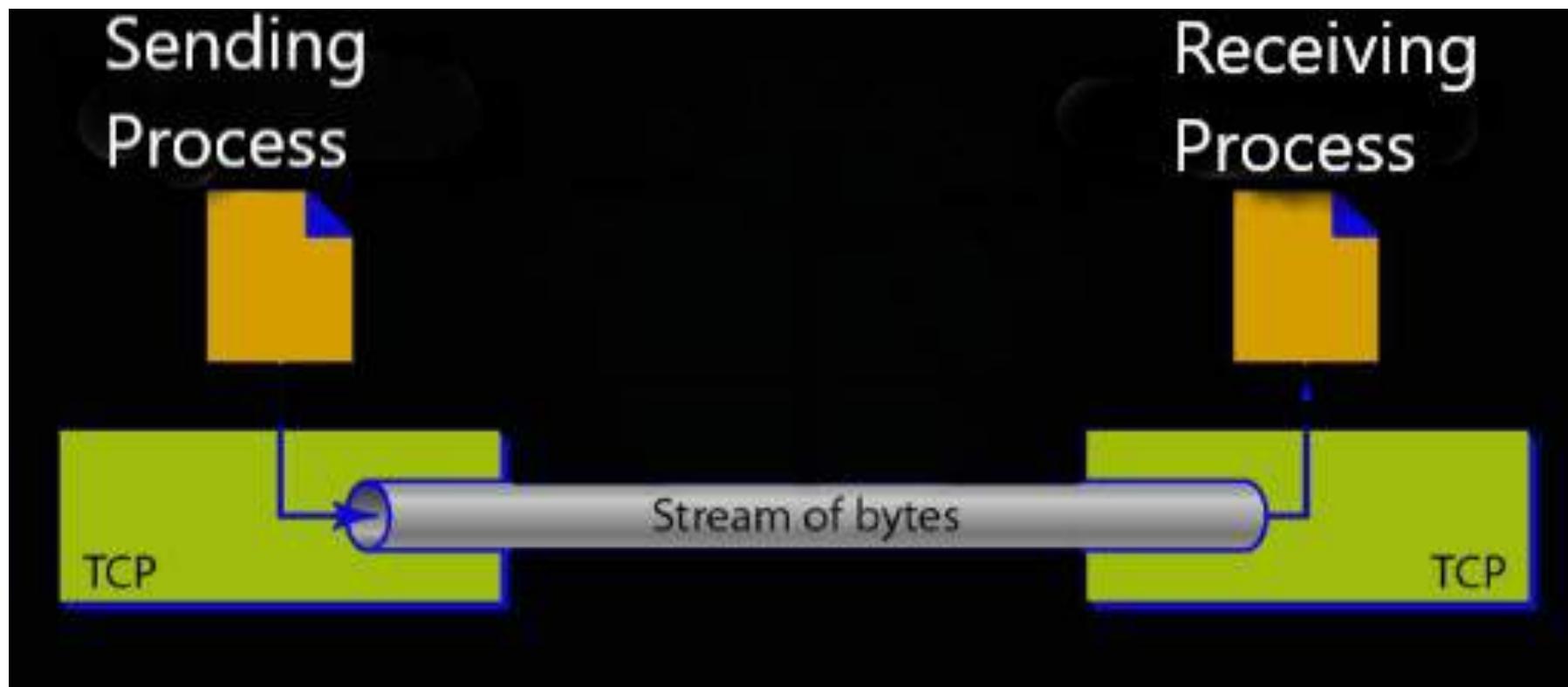
□ Error Control →

□ Congestion control

□ Segmentation and Reassembly

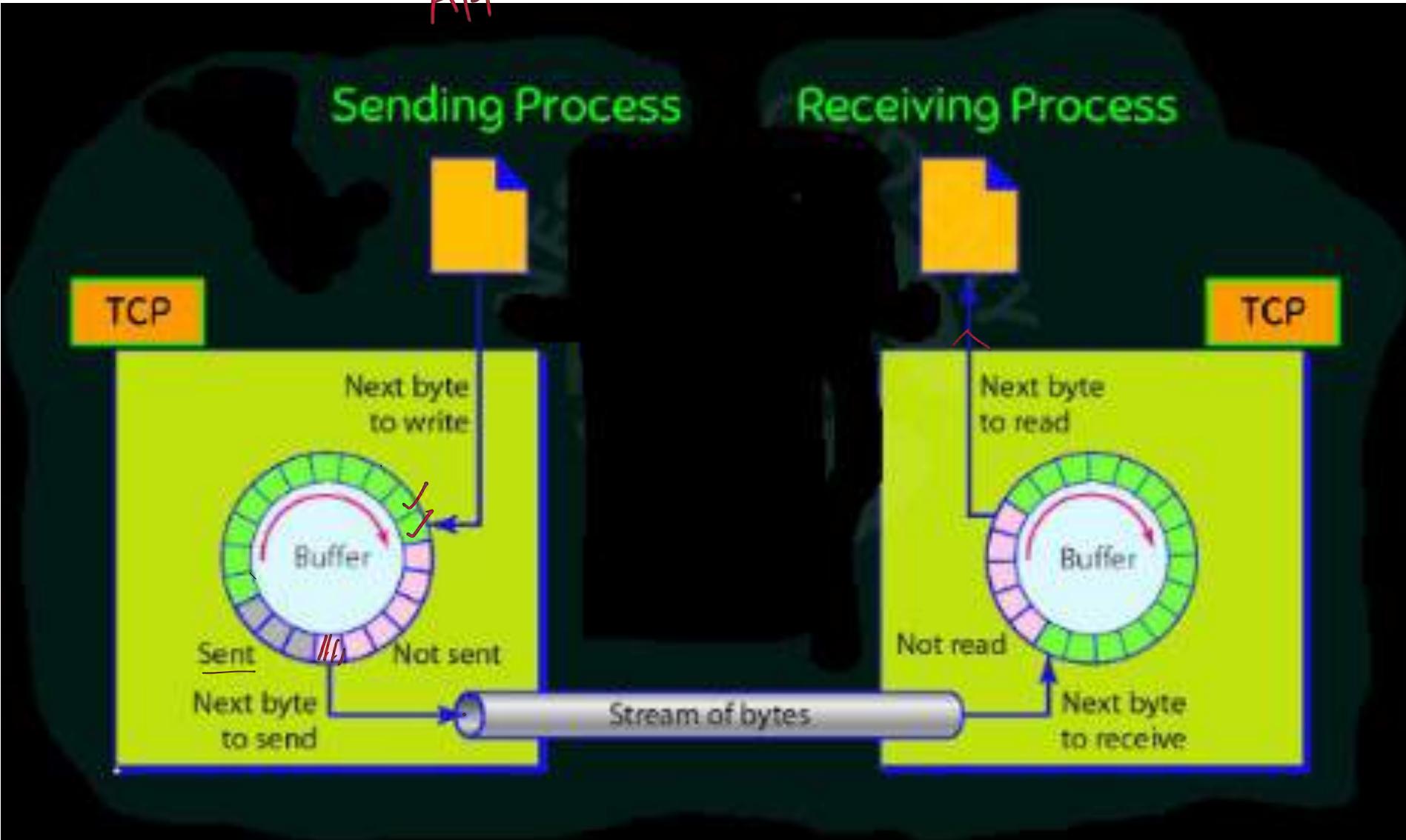
□ Full Duplex Support

TCP Stream Delivery



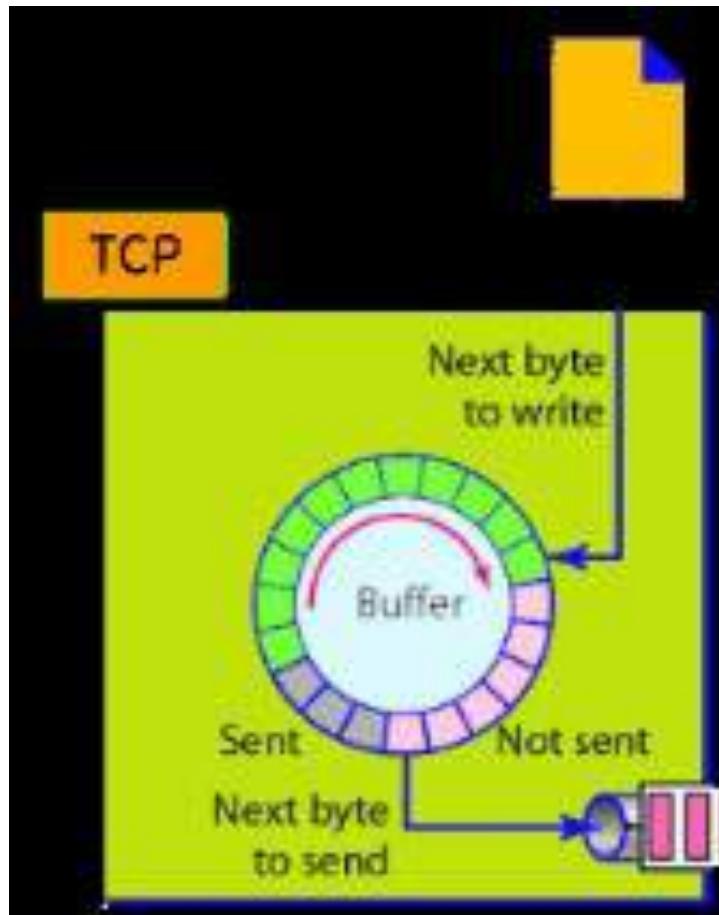
TCP Sending and Receiving Buffers

Application

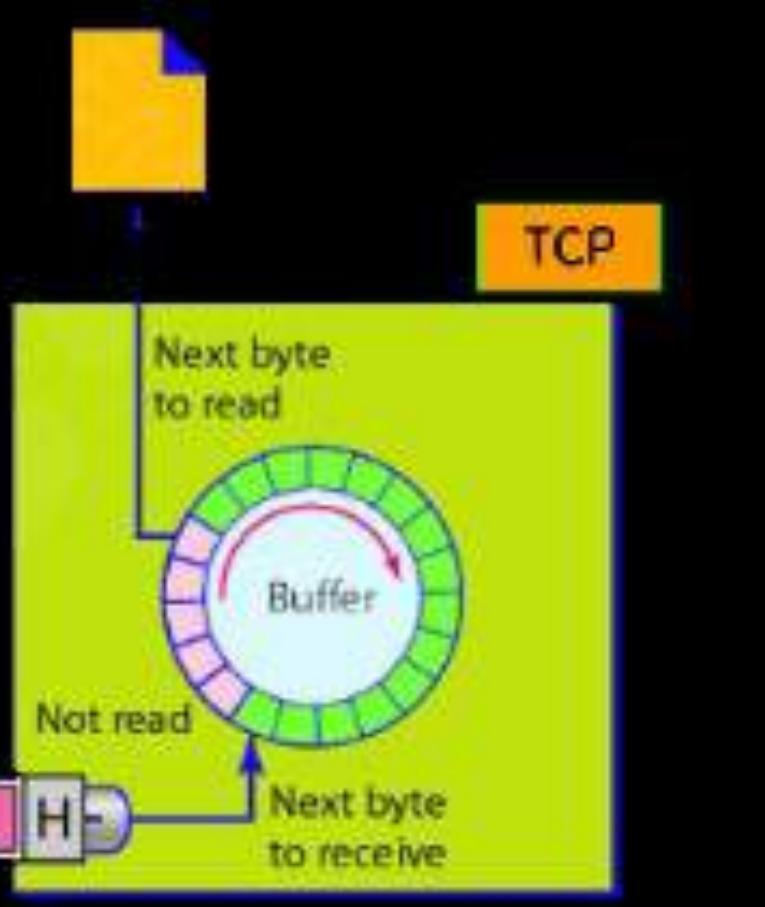


TCP Segments

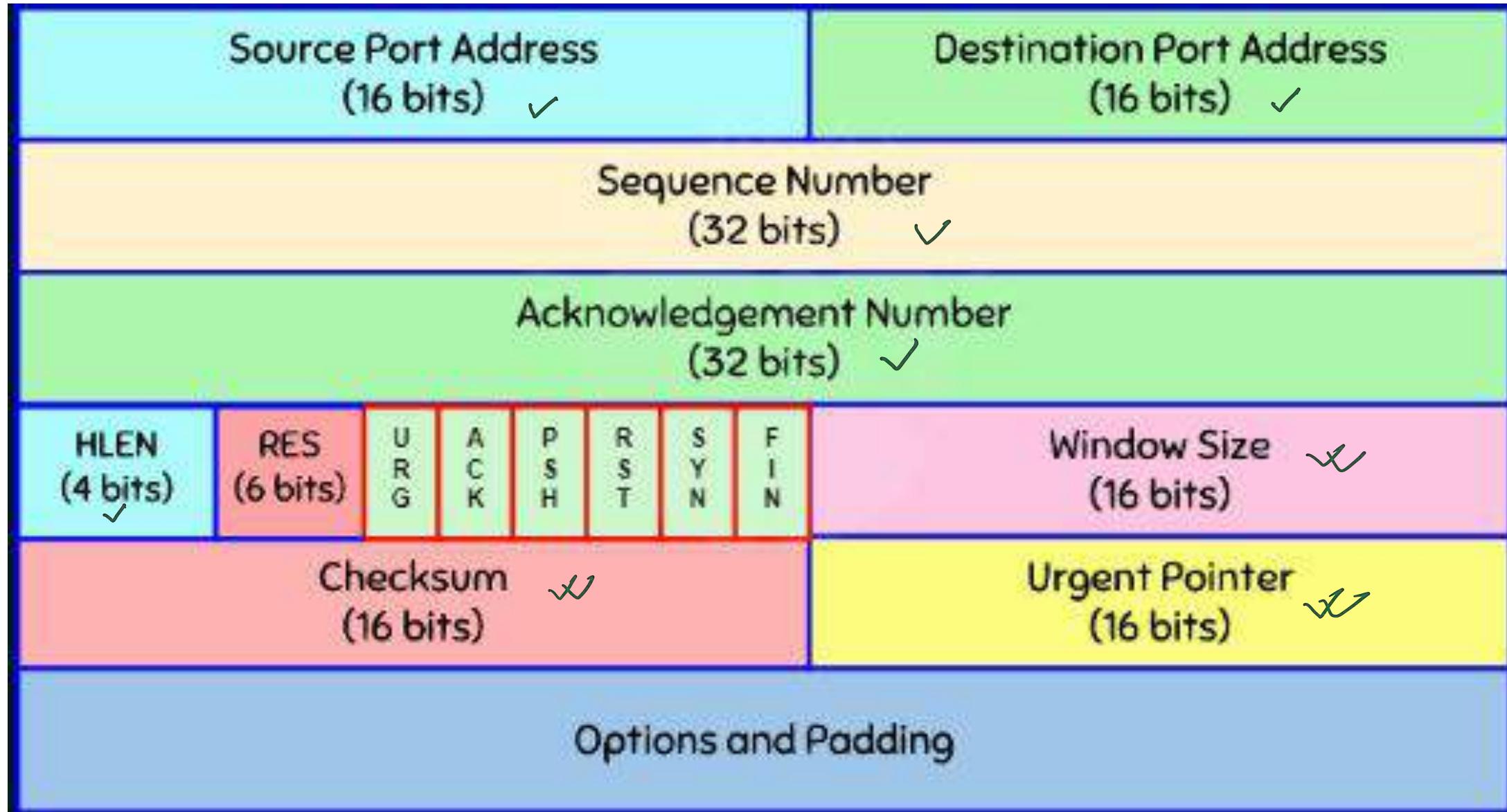
Sending process



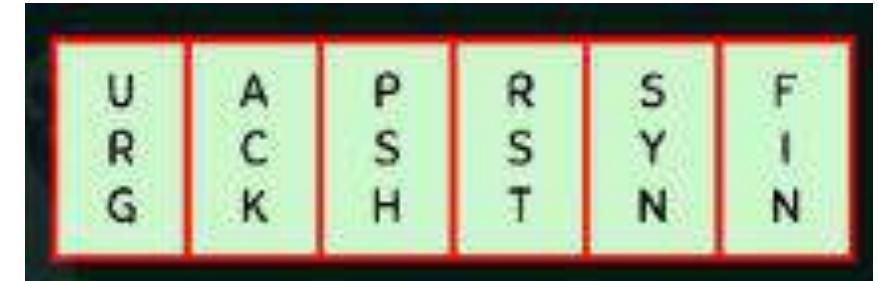
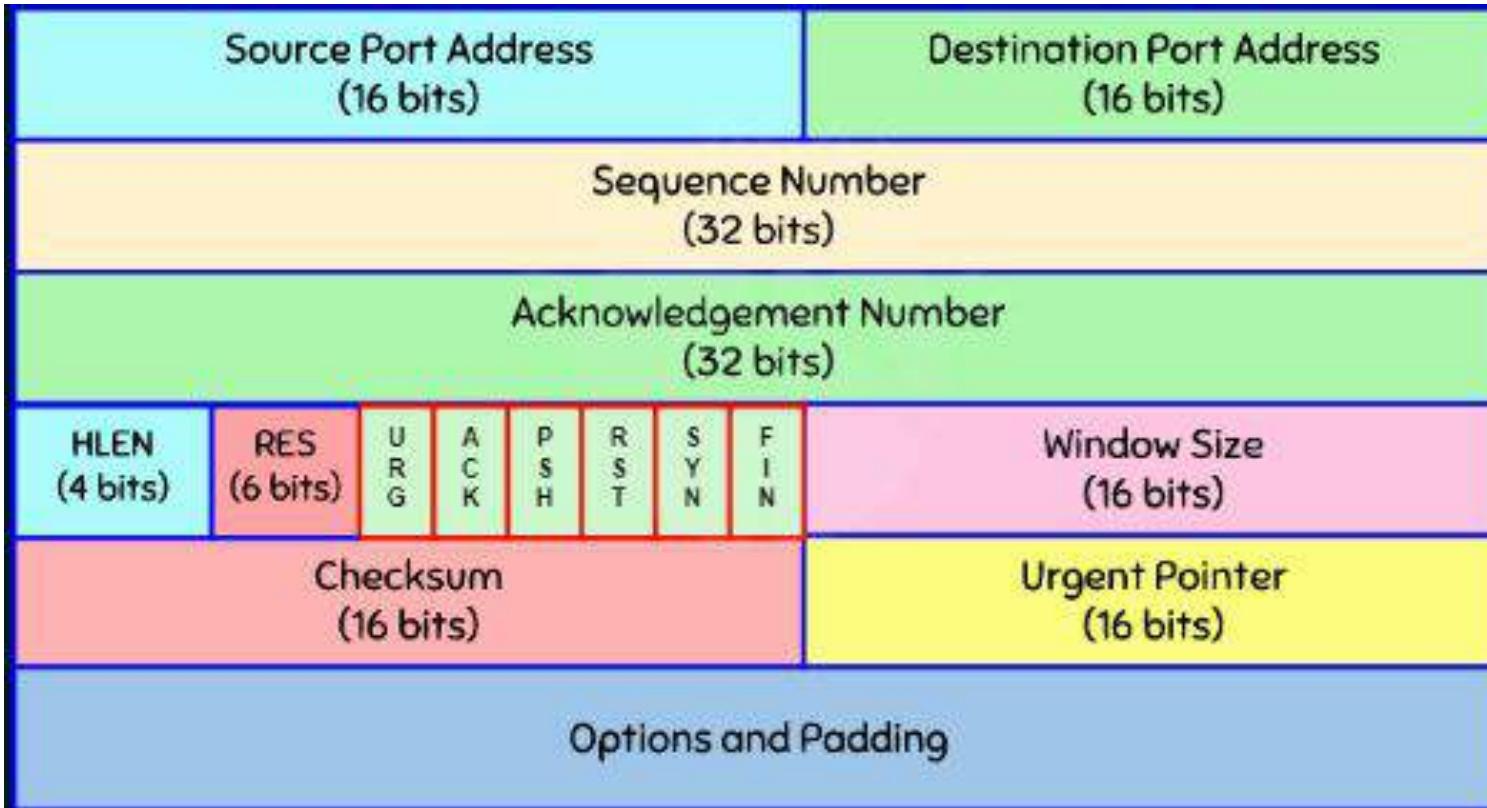
Receiving process



TCP Header Format



TCP Flags

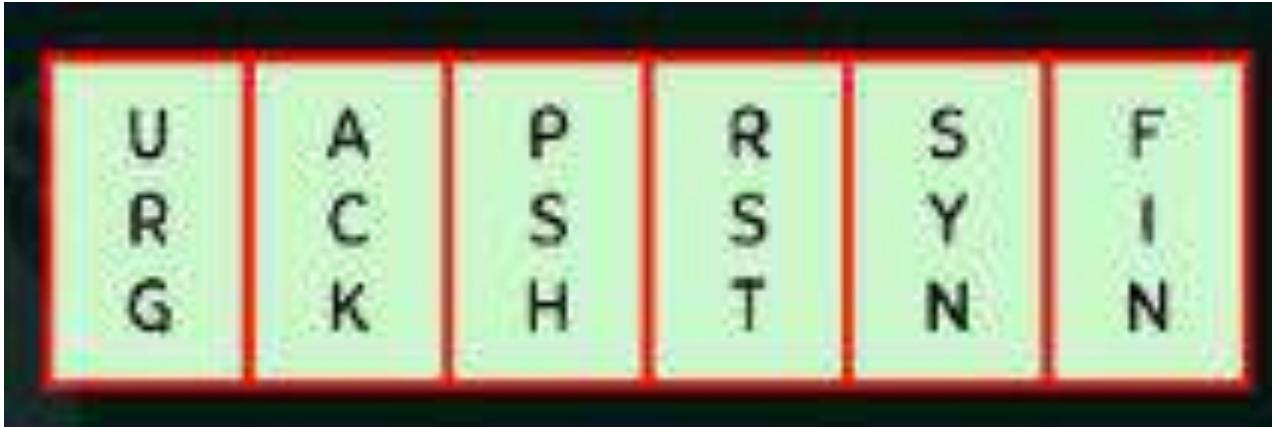


Data
seq₁ seq₂ seq₃

Flag:

- This field defines 6 different control bits or flags.
- One or more of these bits can be set at a time.

TCP Flags



Flag:

- **URG** (1 bit): *Indicates that the Urgent pointer field is significant.*
- **ACK** (1 bit): *Indicates that the Acknowledgement field is significant.*
- **PSH** (1 bit): *Push function. Asks to push the buffered data to the receiving application.*
- **RST** (1 bit): *Reset the connection*
- **SYN** (1 bit): *Synchronize sequence number.*
- **FIN** (1 bit): *Last packet from the sender.*

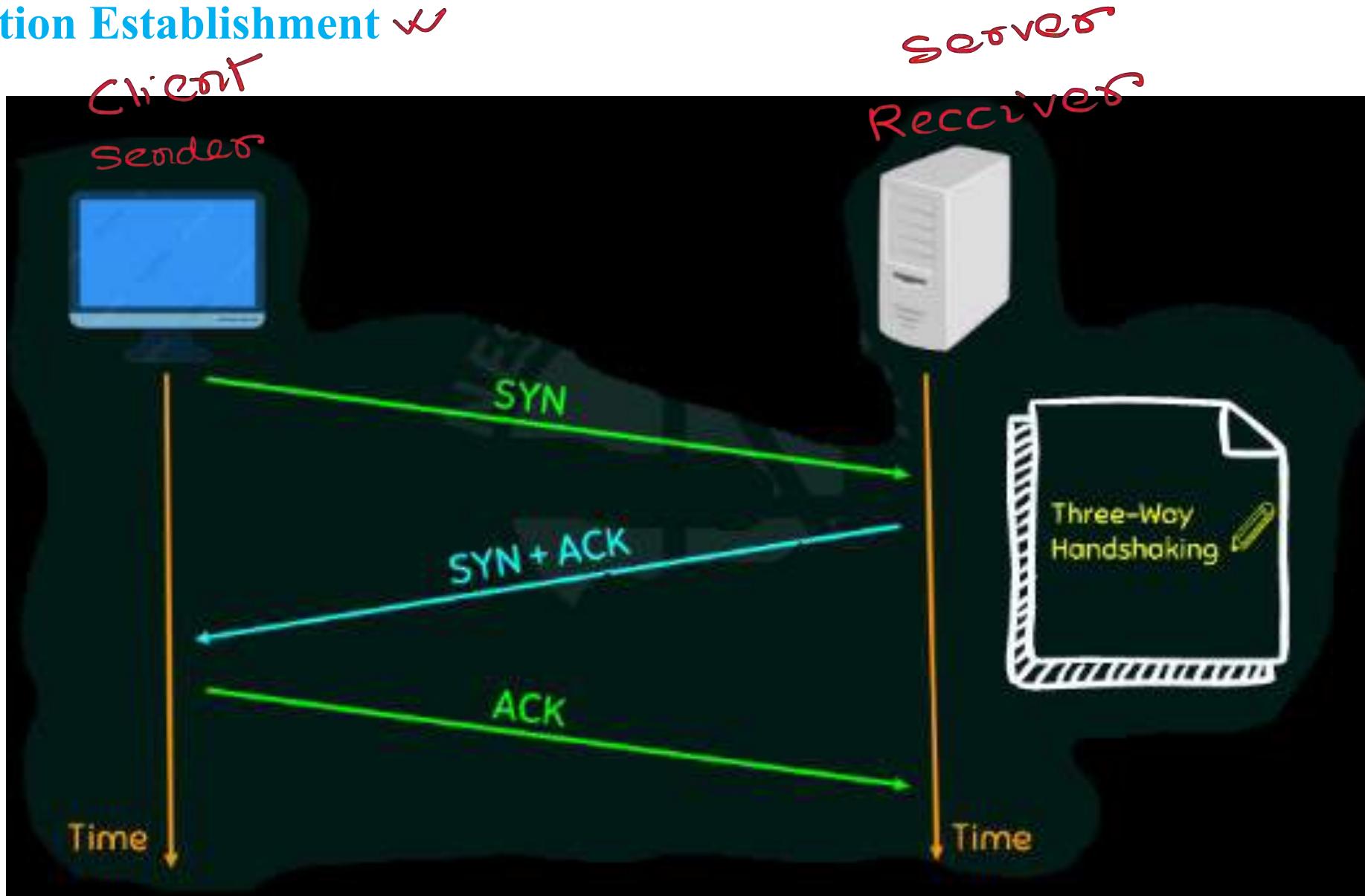
TCP connections

- *Connection oriented.*
- *Virtual path.*
- *Acknowledgement process.*
- *RST (1 bit): Reset the connection*
- *Retransmission of lost or damaged segments.*
- *TCP connection-Virtual not physical.*
- *IP –connection*
- *Full-duplex mode.*
- *Approval from other party.*

Three Phases of TCP connections

- *Connection Establishment* ✓
- *Data Transfer* ✓
- *Connection Termination* ✓

TCP Connection Establishment ✓

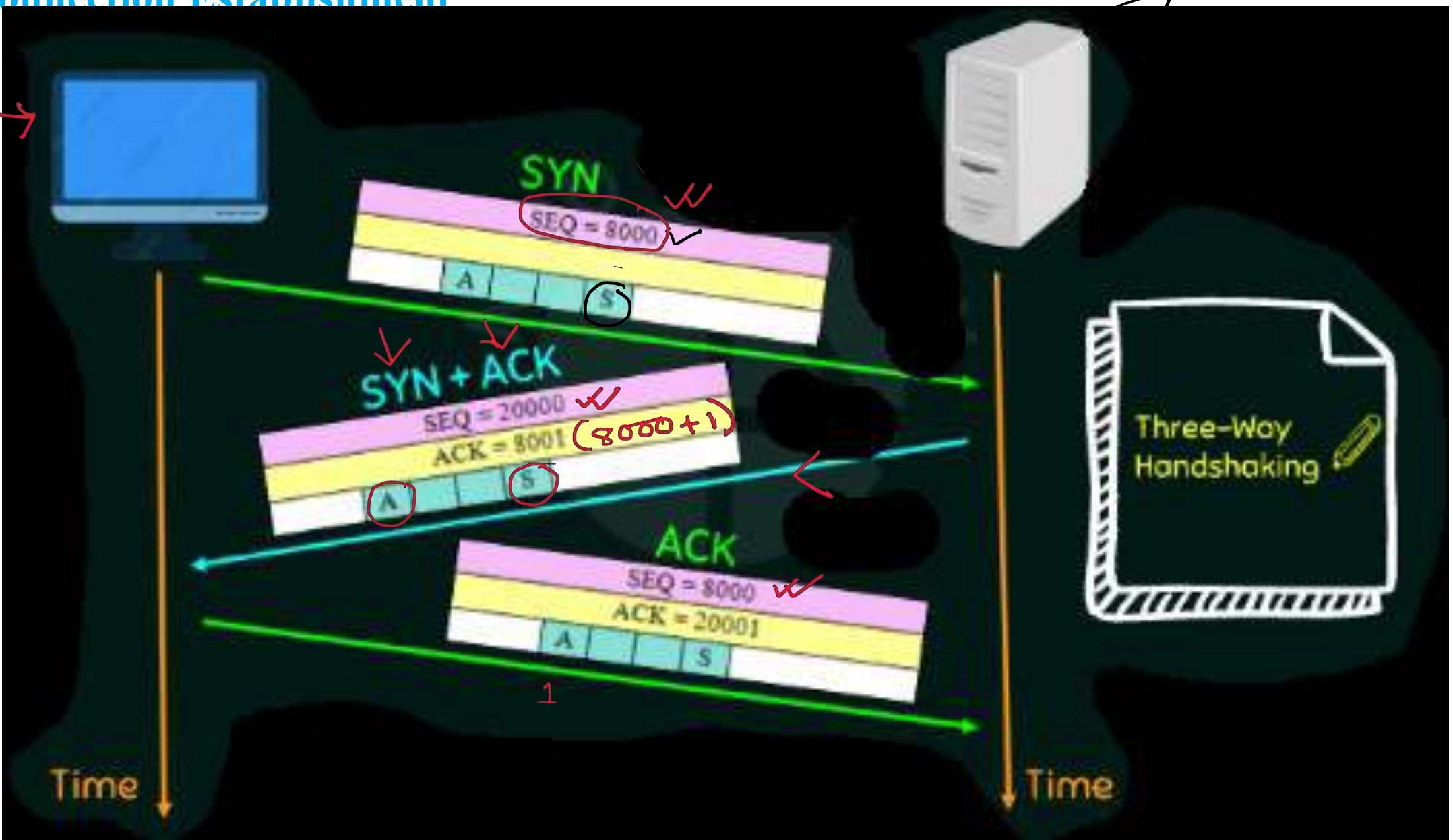


TCP Connection Establishment

sequence

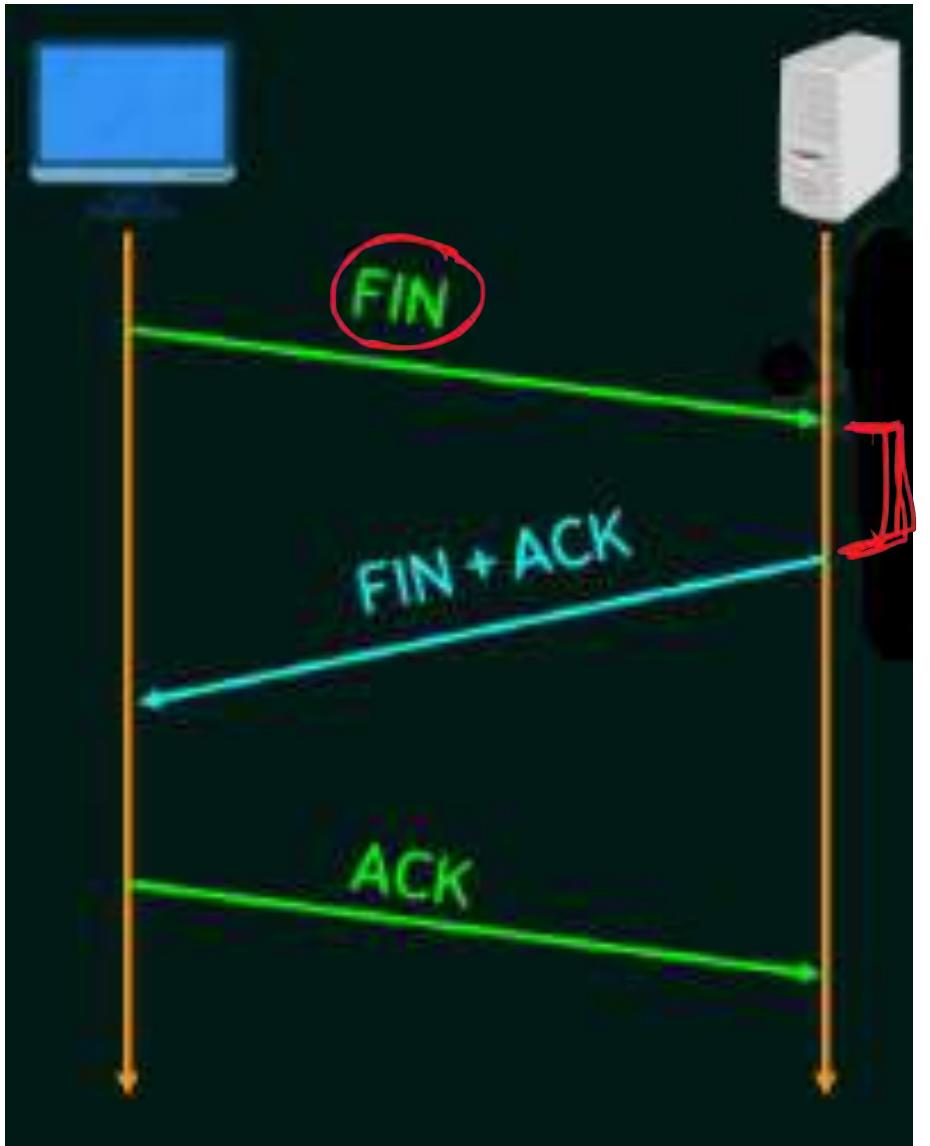
numbers

client
seq no

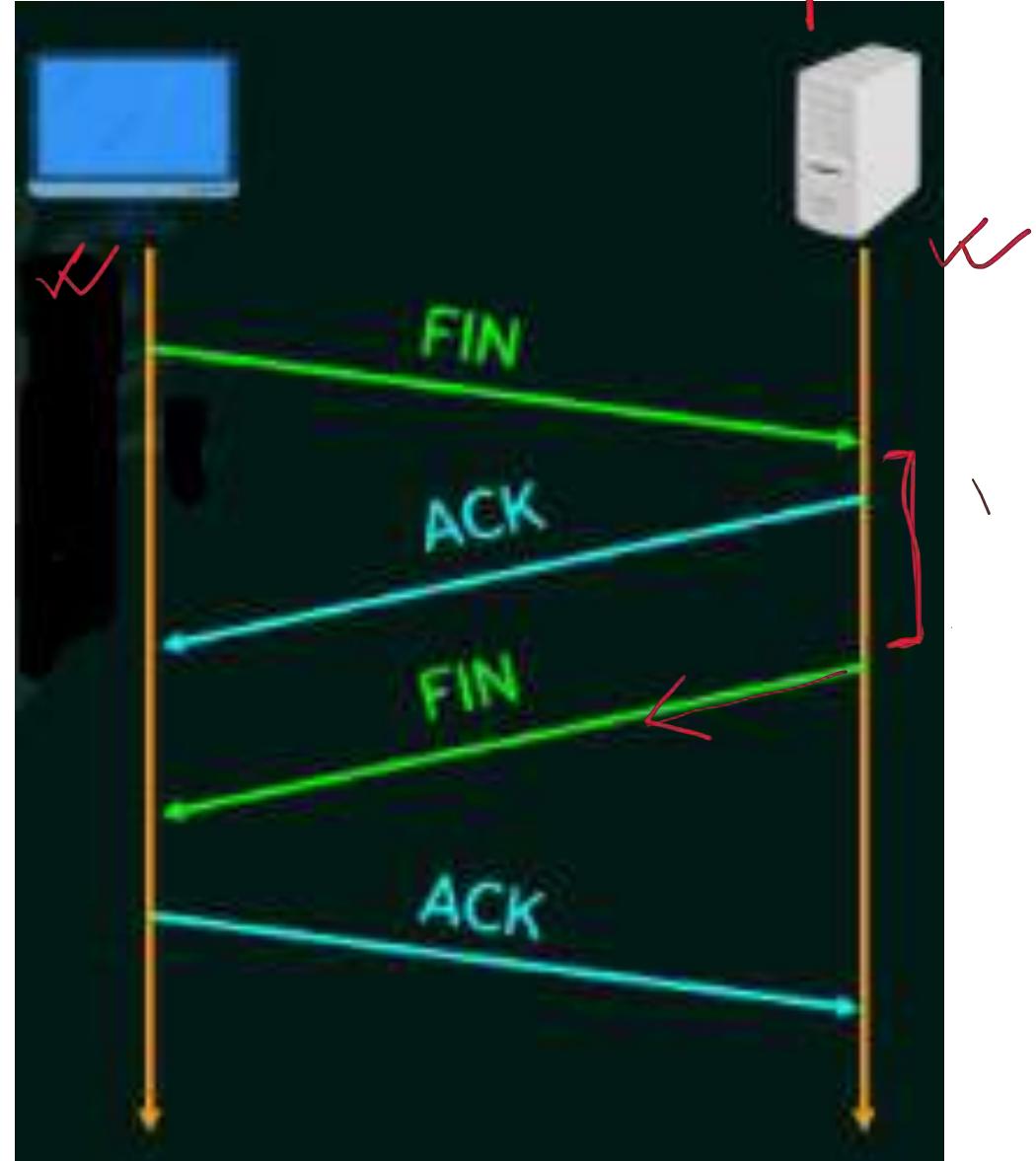


TCP Connection Termination

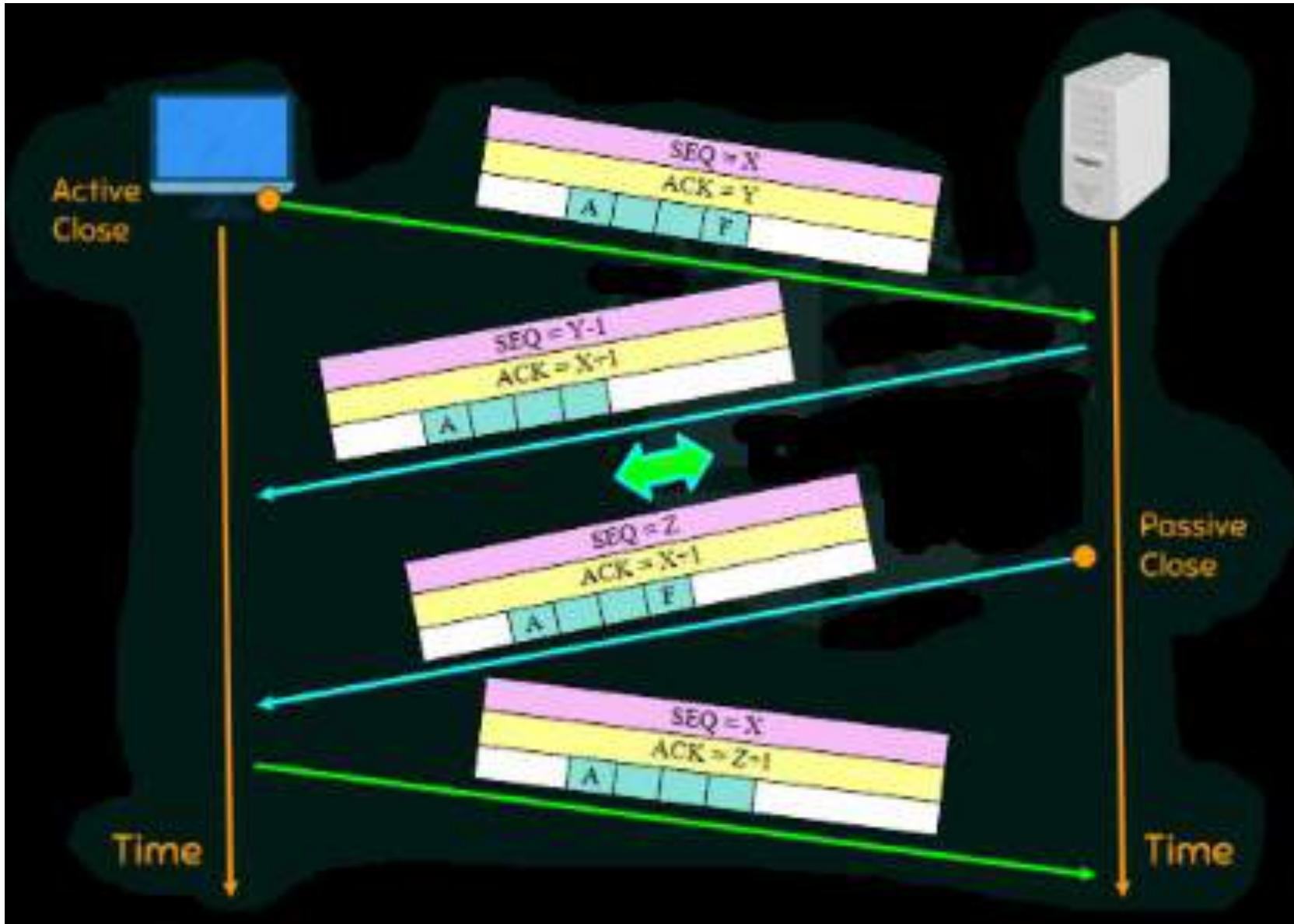
Three-way



Four-way

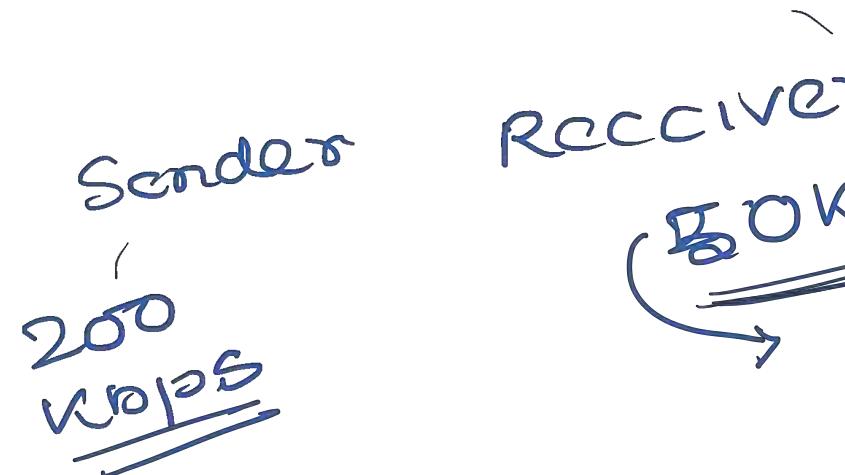


Connection Termination



TCP Flow Control

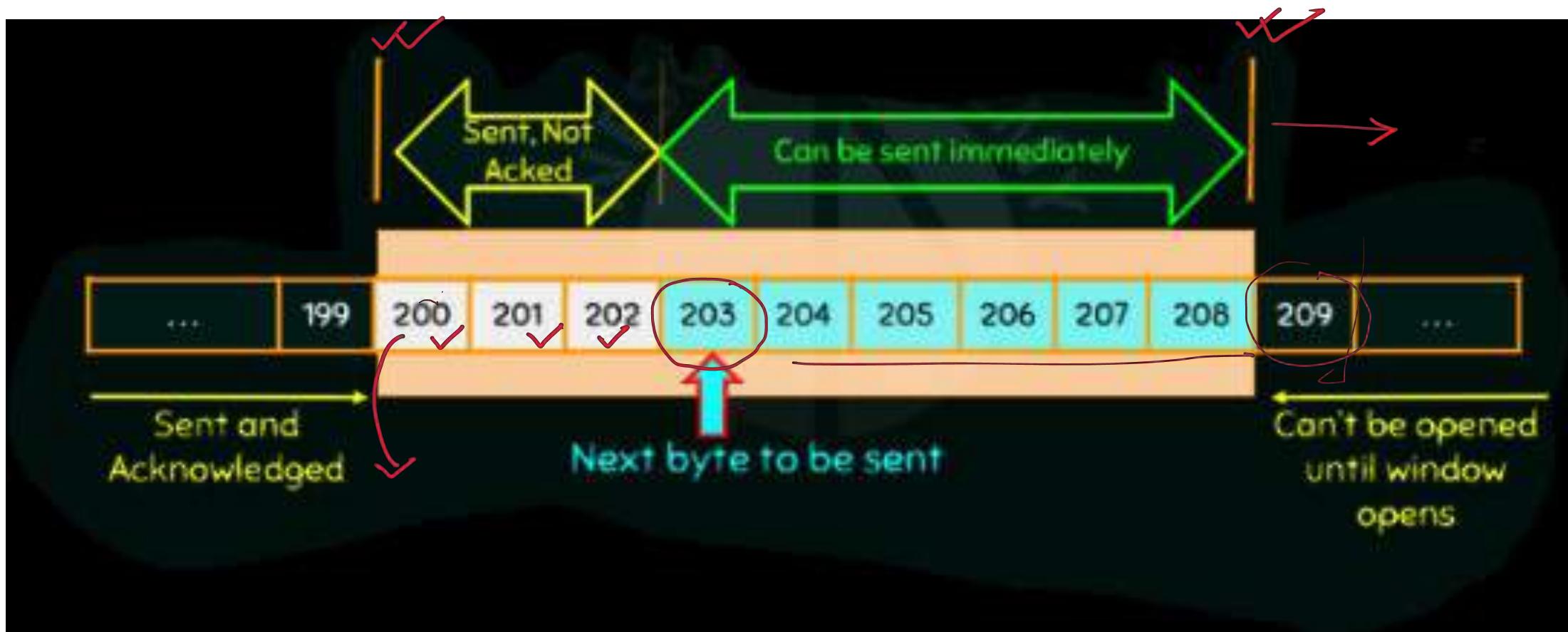
- TCP uses a sliding window to handle flow control. ✓
- Between Go-back and selective Repeat.
- Does not use NAK.
- The receiver holds out-of-order segments.
- TCP sliding window is byte-oriented. ✓
- TCP's sliding window is of variable size. ✓
- Imaginary window. ✓



TCP Sliding Window

200 kbps Sender

✓ ✓
Window size = Minimum (rwnd, cwnd) = Minimum (20,9) = 9

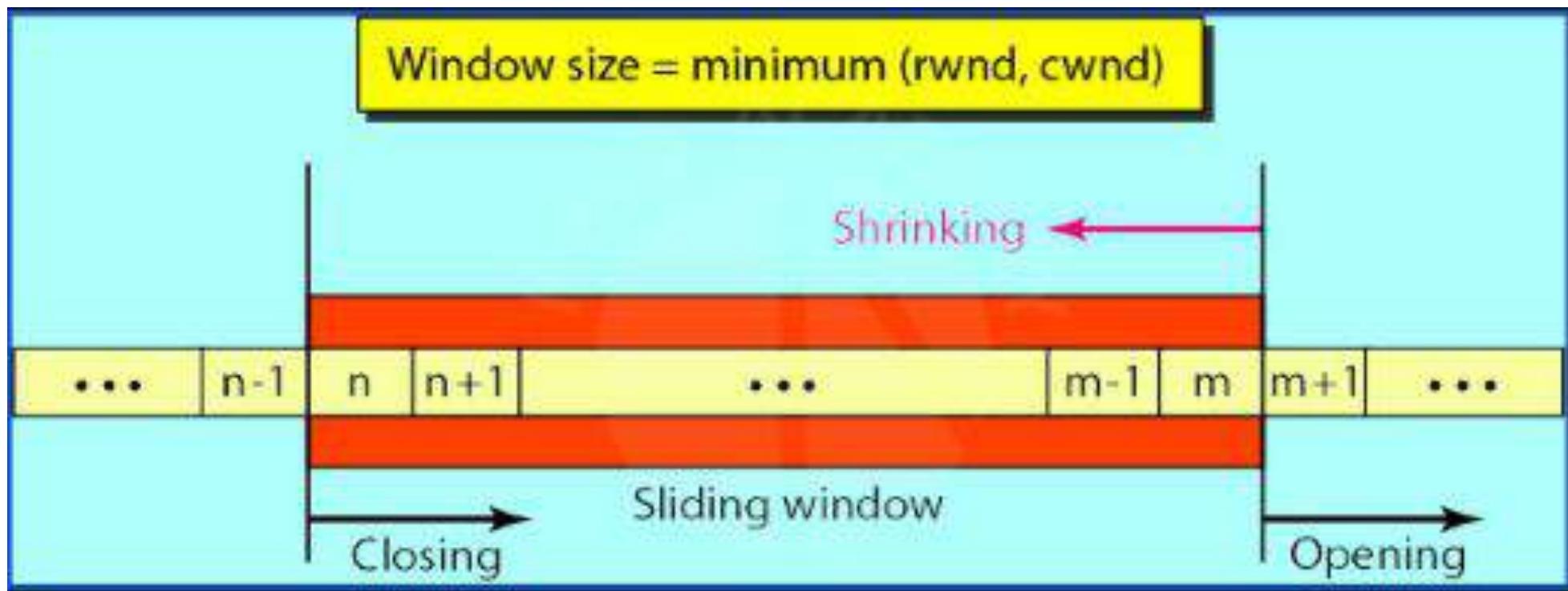


TCP Sliding Window

Points to remember

- ◻ Window size = Minimum (rwnd, cwnd). ✓ ✓
- ◻ The source does not have to send a full window's worth of data.
- ◻ The window can be opened or closed by the receiver, but should not be shrunk.
- ◻ The destination can send an ACK at any time
- ◻ The sender can send 1-byte segment even after the window is shut down in the receiver side.

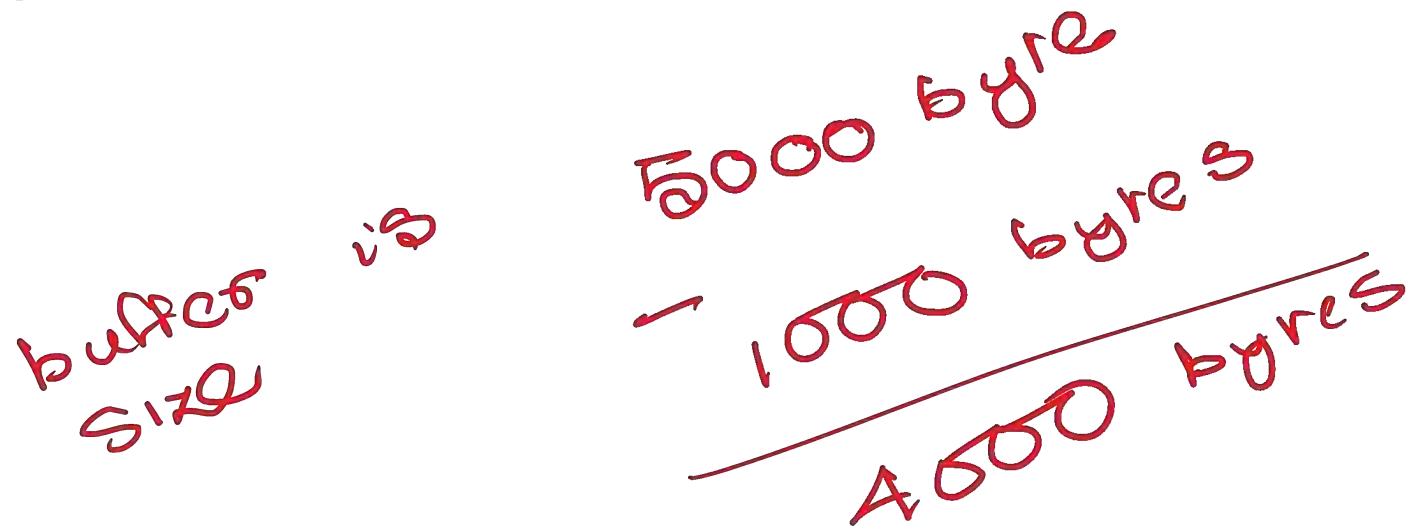
TCP Sliding Window



Questions. What is the value of the receiver window (rwnd) for host A if the receiver host B, has a buffer size of 5000 bytes and 1000 bytes of received and unprocessed data.

$$\text{Rwnd} = 5000 - 1000 = 4000 \text{ bytes}$$

Host B can only receive bytes of data before overflowing its buffer. Host B advertises this value 4000 in its next segment to Host A.



Questions. Suppose a TCP connection is transferring a file of 1000 bytes, The first byte is numbered 100001. What is the sequence number of the segment if all data is sent in only one segment?

File size = 1000 bytes

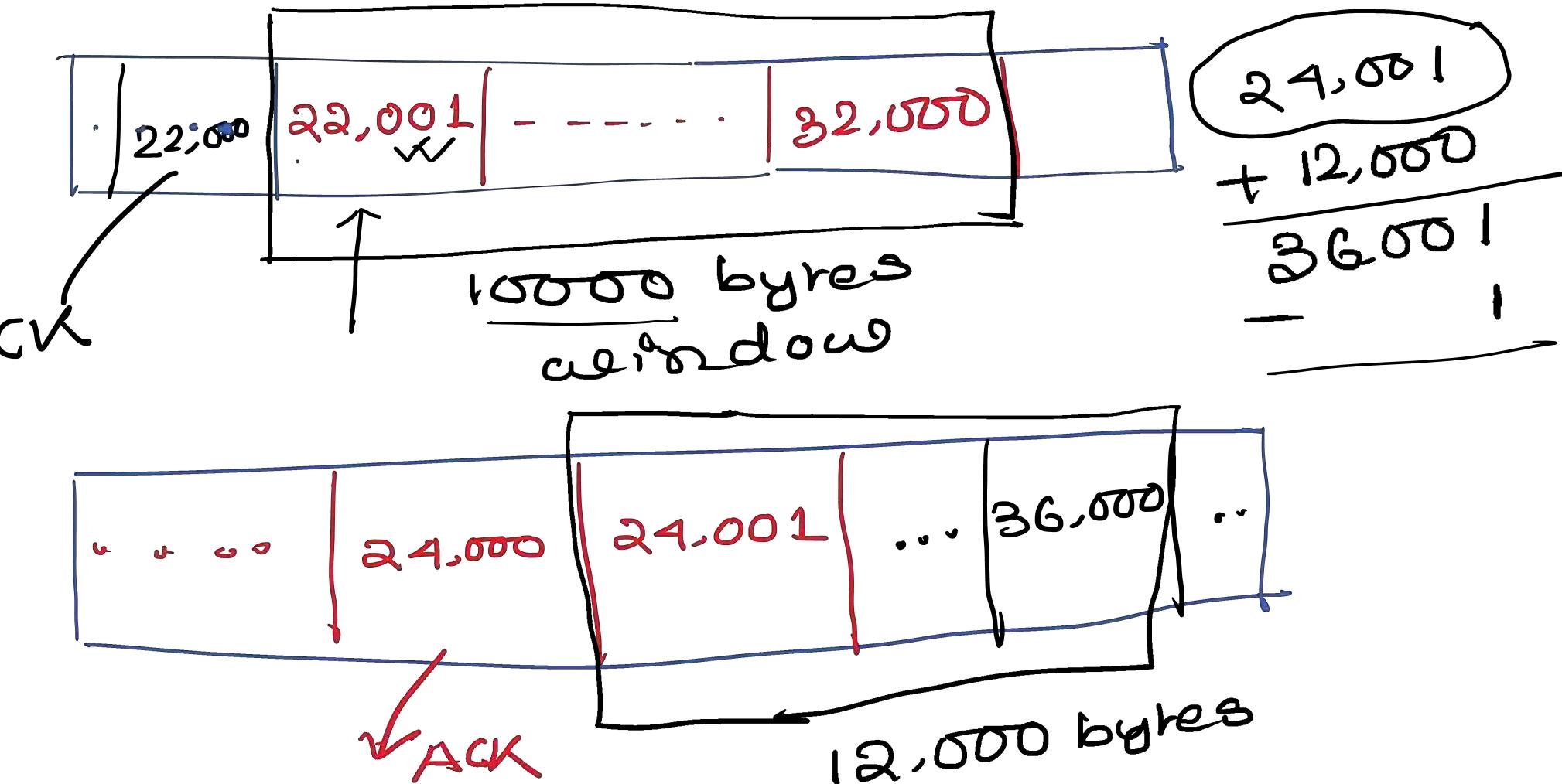
First byte of data = 10,000 + 1
+ 1000

101001 bytes

- 1

101000 bytes

Questions. A TCP connection is using a window size of 10,000 bytes, and the previous acknowledgement number was 22,001. It receives a segment with acknowledgement number 24,001 and window size advertisement of 12,000. Draw a diagram to show the situation of the window before and after.



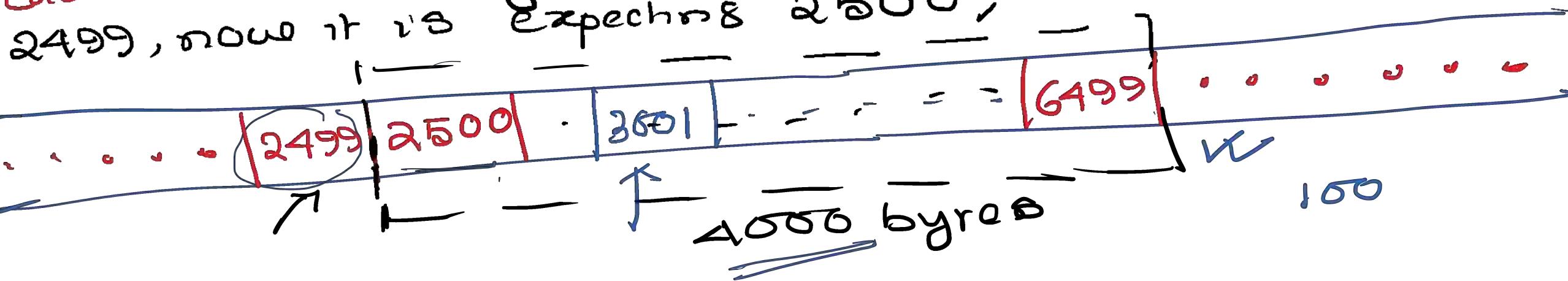
Questions. A window holds bytes 2001 to 5000. The next byte to be sent is 3001. Draw a figure to show the situation of the window after the following two events.

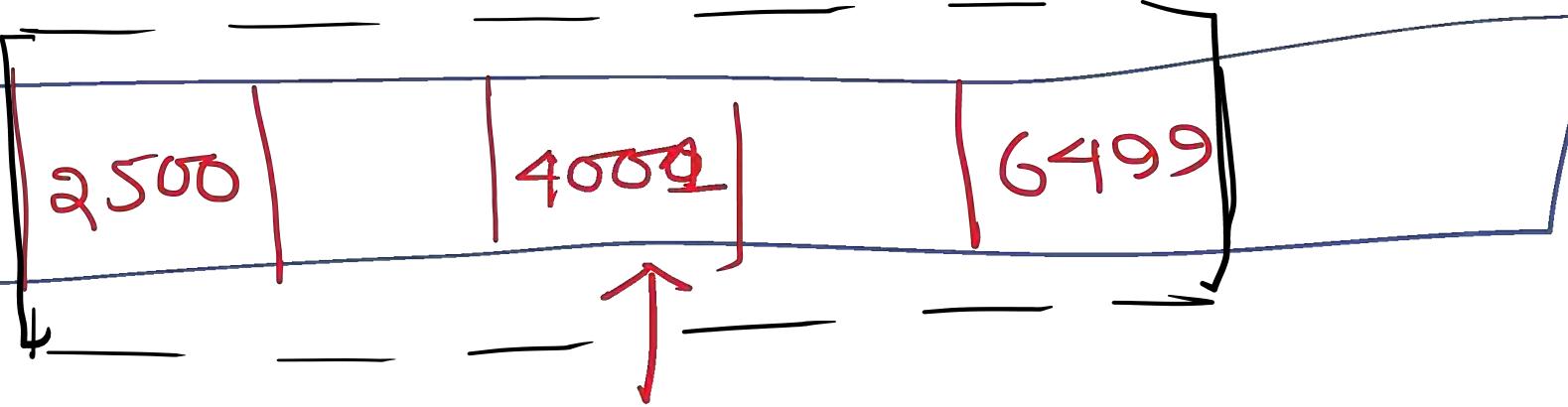
- a. An ACK segment with the acknowledgement number 2500 and window size advertisement 4000 is received. ✓

- b. A segment carrying 1000 bytes is sent. ✓



Case 1:- successfully received the segment with seq no 2499, now it's expecting 2500, window = 4000





next
byte
to be sent

3001
↑
1000 bytes

$$\begin{array}{r} 30 \\ \rightarrow 10 \\ \hline 40 \end{array}$$

Module 4

Transport Layer



Dr. Sunandita Debnath, IIIT Vadodara

TCP

Features of TCP

□ Connection oriented

□ Reliable delivery ✓

□ Acknowledgement oriented

□ Retransmission

□ Flow control ✓

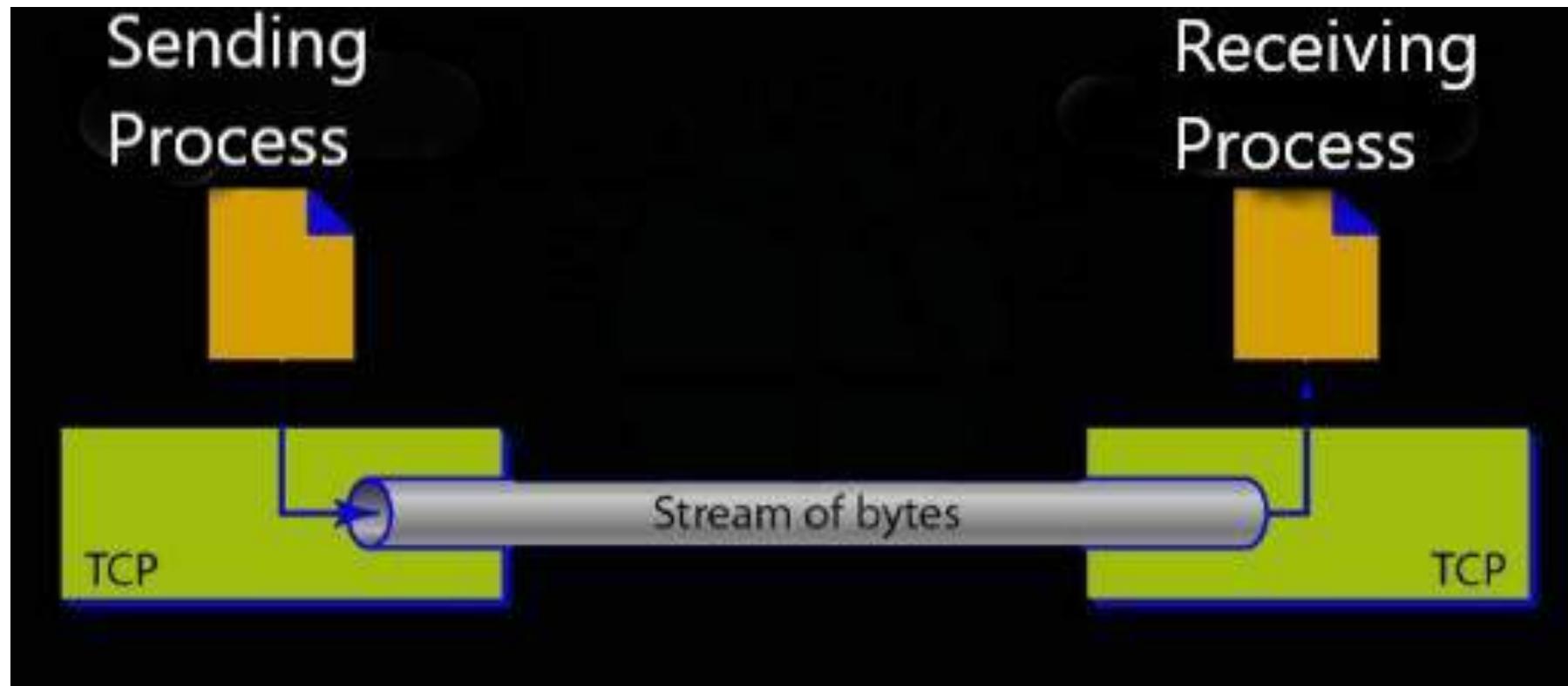
□ Error Control →

□ Congestion control

□ Segmentation and Reassembly

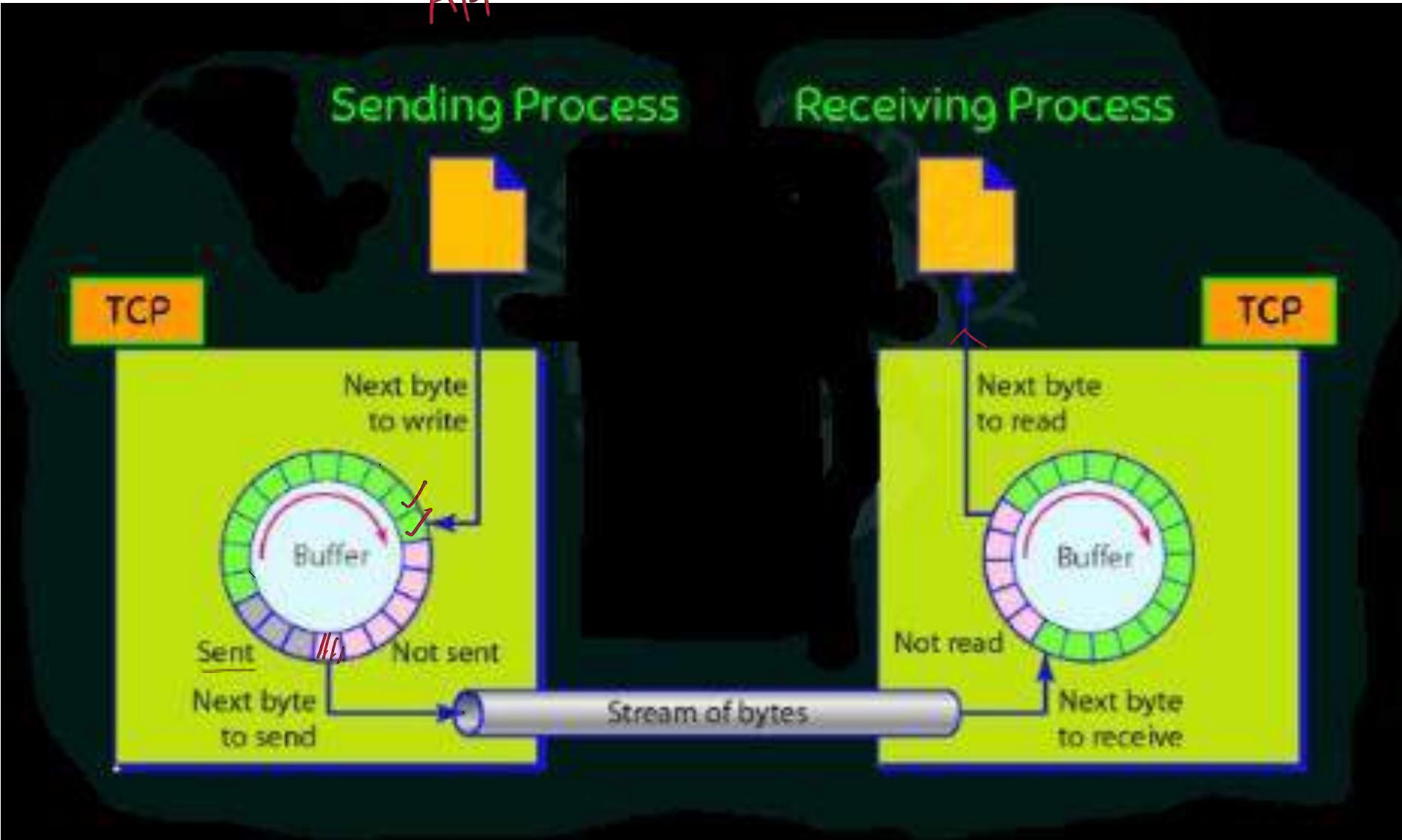
□ Full Duplex Support

TCP Stream Delivery



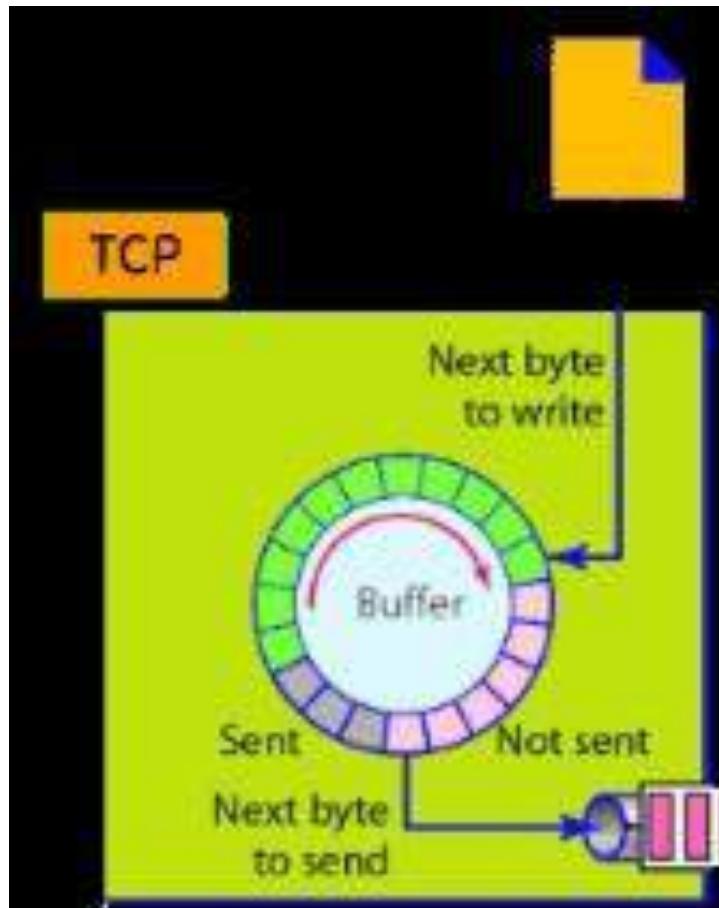
TCP Sending and Receiving Buffers

Application

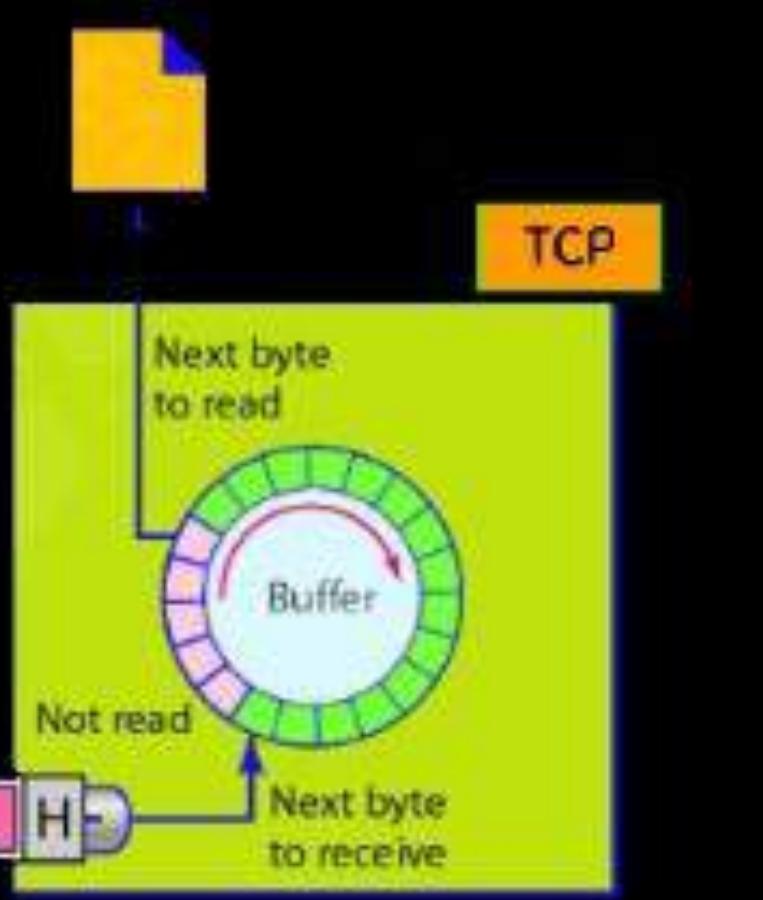


TCP Segments

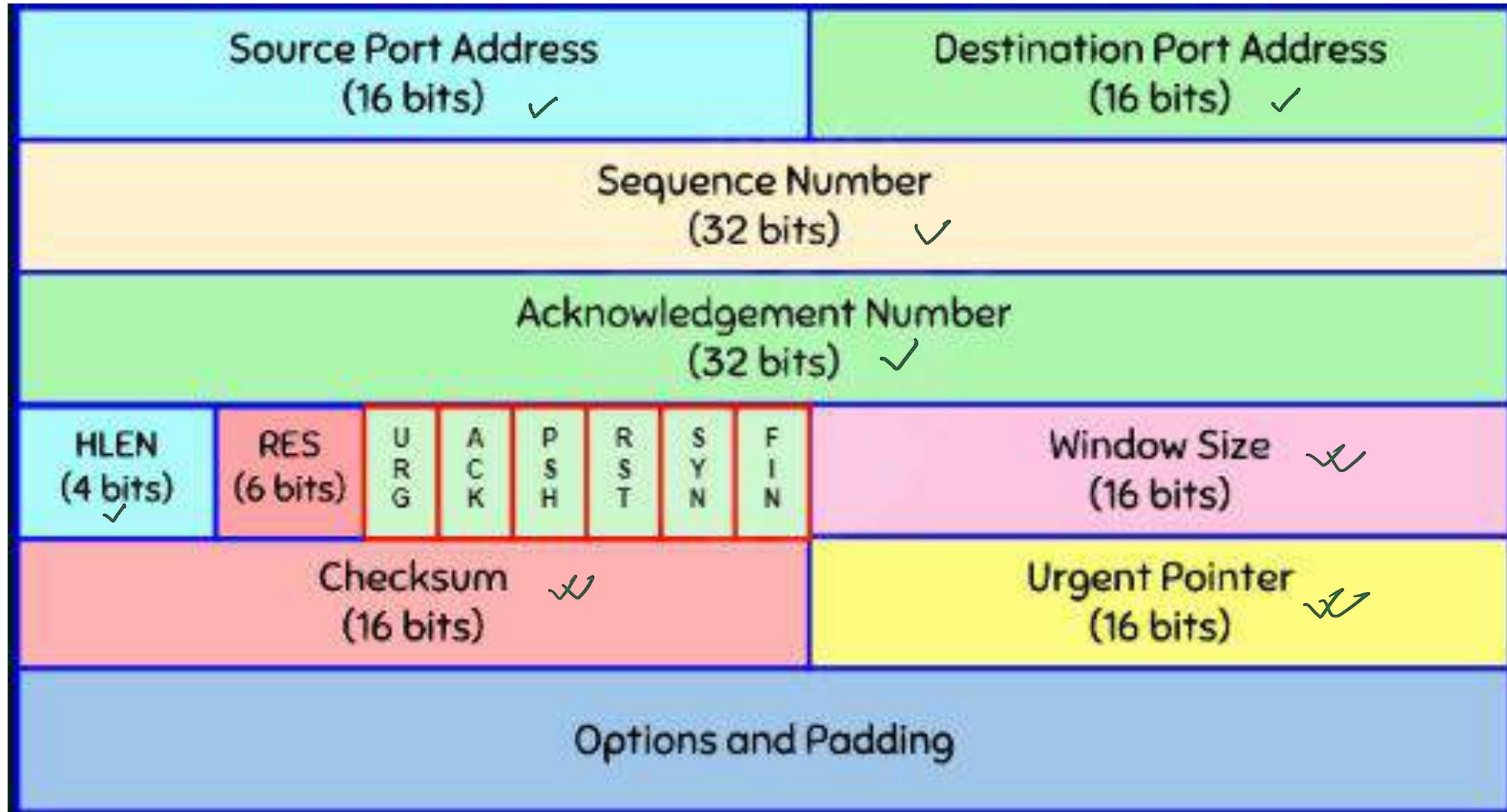
Sending process



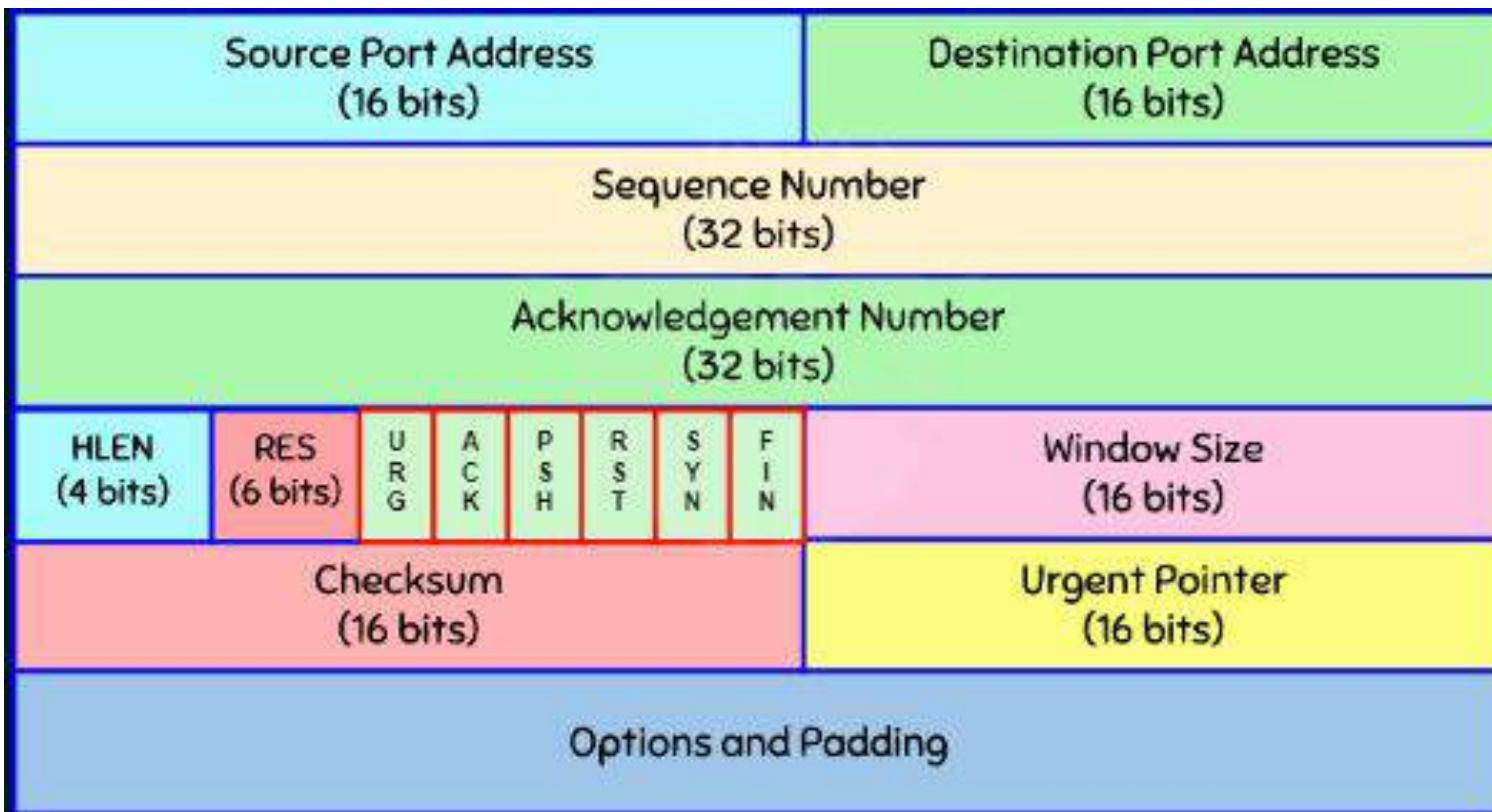
Receiving process



TCP Header Format



TCP Flags



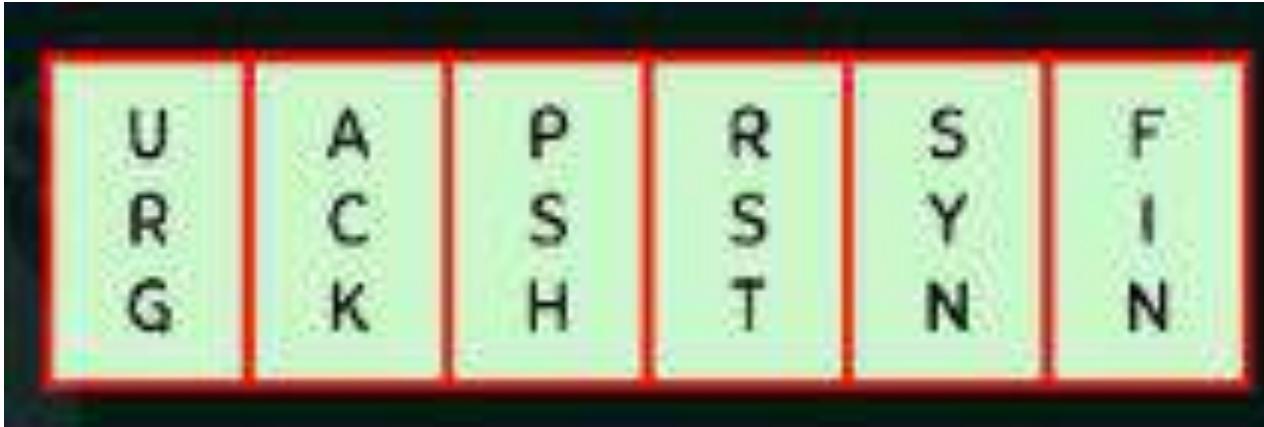
1 1 1 1 1 1

Data
seq₁ seq₂ seq₃

Flag:

- This field defines 6 different control bits or flags.
- One or more of these bits can be set at a time.

TCP Flags



Flag:

- **URG** (1 bit): *Indicates that the Urgent pointer field is significant.*
- **ACK** (1 bit): *Indicates that the Acknowledgement field is significant.*
- **PSH** (1 bit): *Push function. Asks to push the buffered data to the receiving application.*
- **RST** (1 bit): *Reset the connection*
- **SYN** (1 bit): *Synchronize sequence number.*
- **FIN** (1 bit): *Last packet from the sender.*

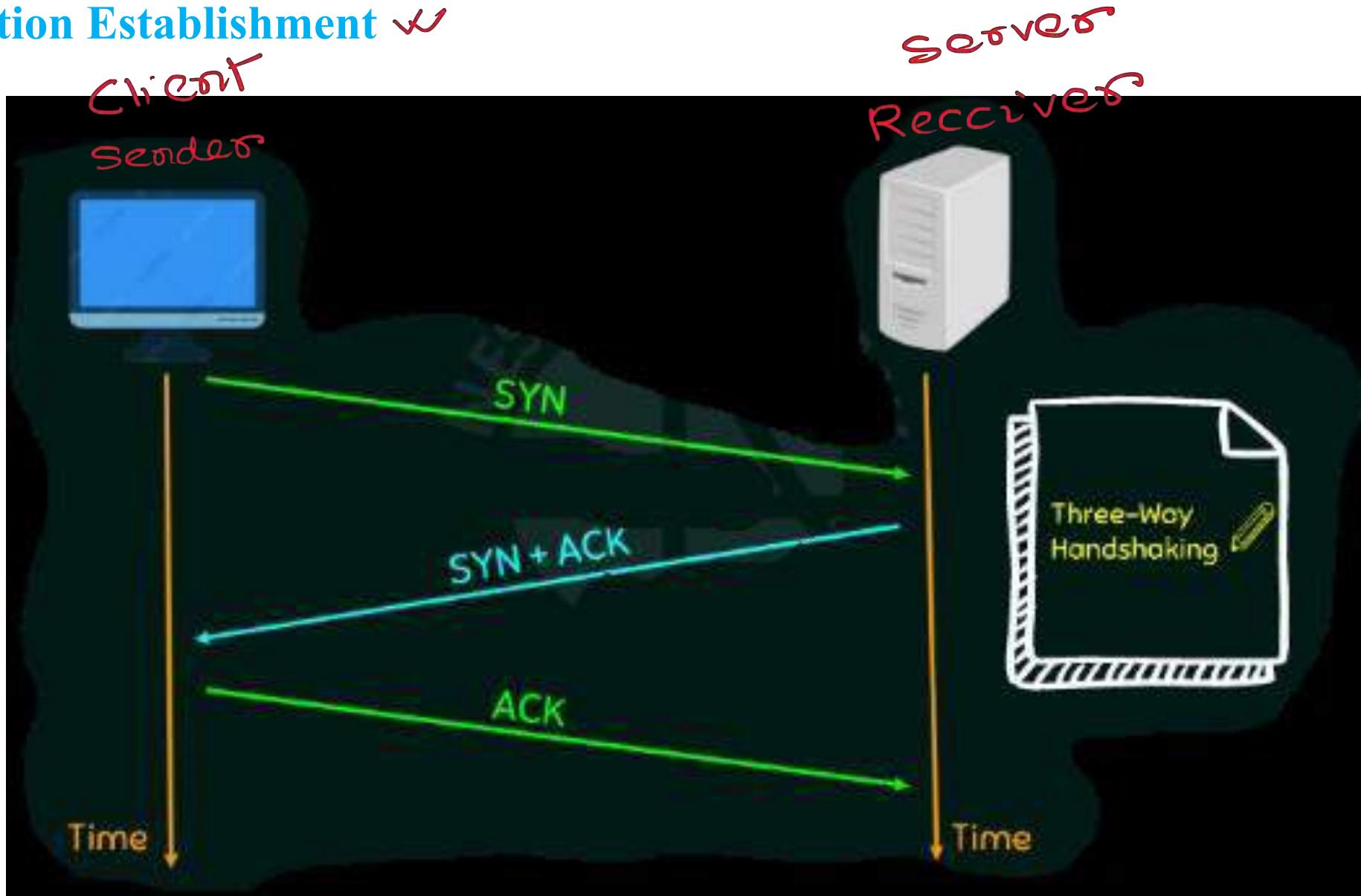
TCP connections

- *Connection oriented.*
- *Virtual path.*
- *Acknowledgement process.*
- *RST (1 bit): Reset the connection*
- *Retransmission of lost or damaged segments.*
- *TCP connection-Virtual not physical.*
- *IP –connection*
- *Full-duplex mode.*
- *Approval from other party.*

Three Phases of TCP connections

- *Connection Establishment* ✓
- *Data Transfer* ✓
- *Connection Termination* ✓

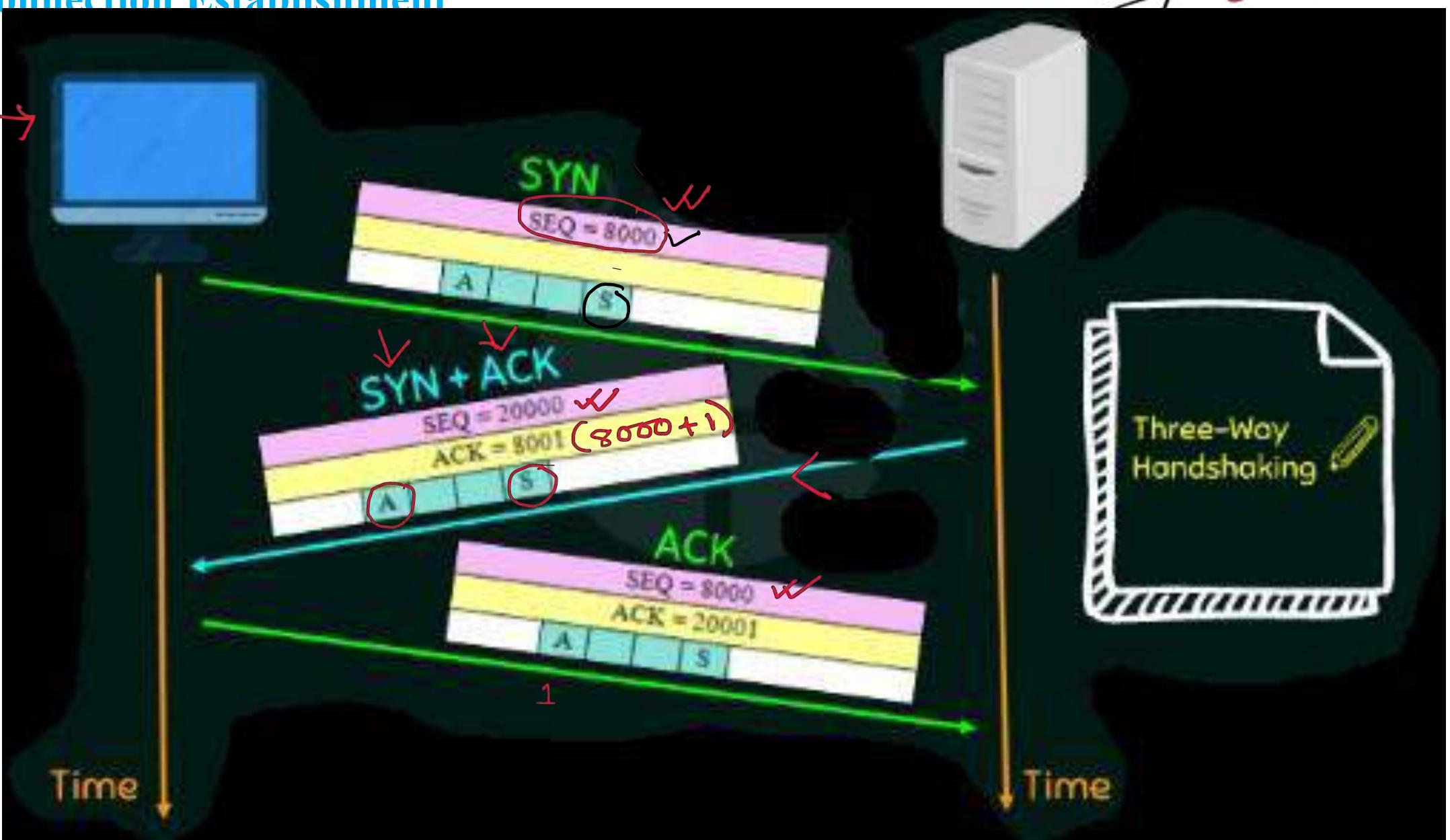
TCP Connection Establishment ✓



TCP Connection Establishment

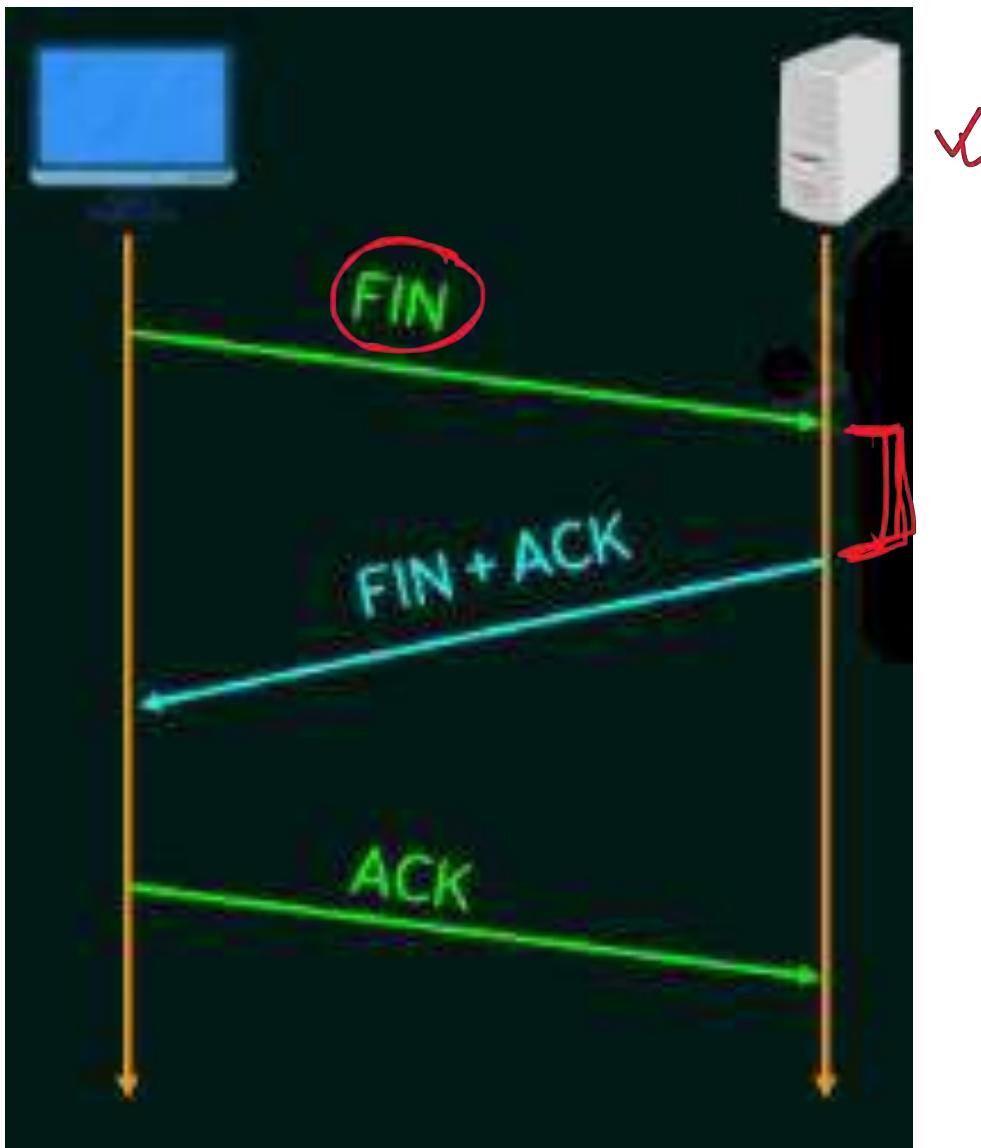
sequence
numbers

initial
seq no

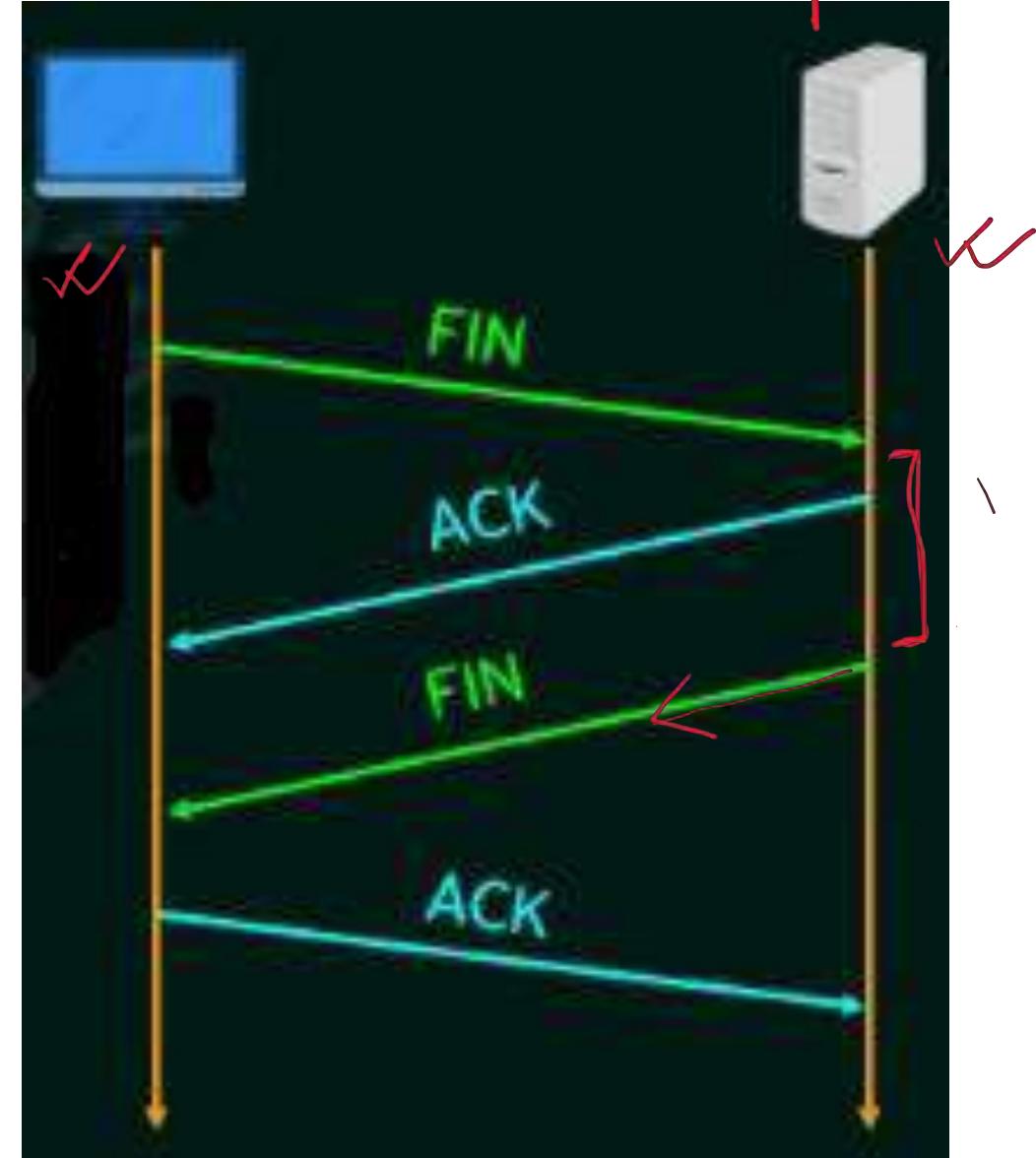


TCP Connection Termination

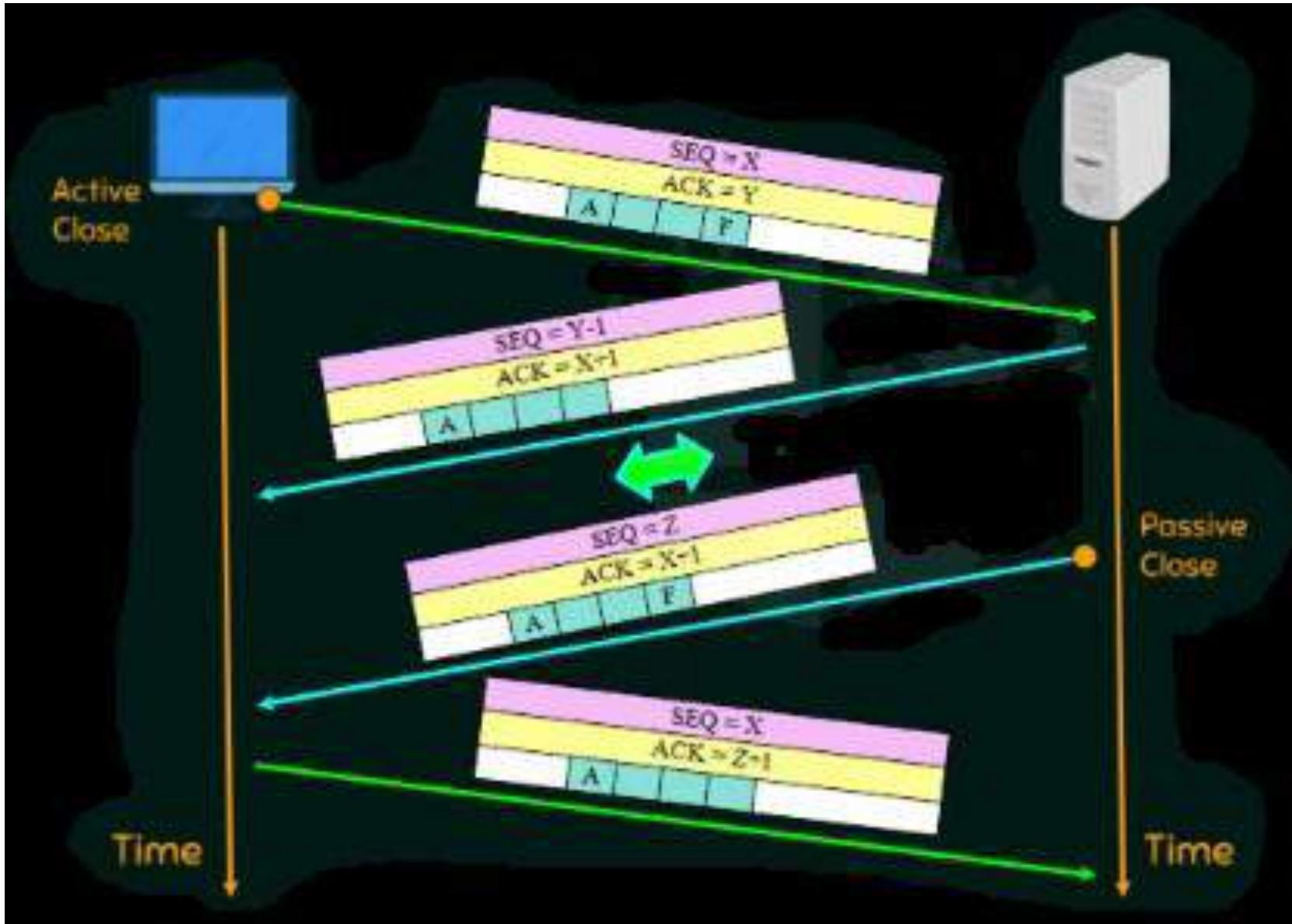
Three-way



Four-way

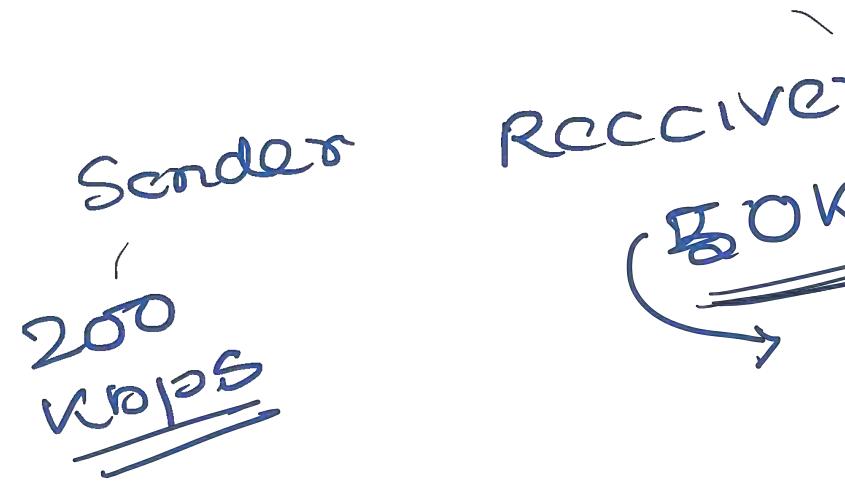


Connection Termination



TCP Flow Control

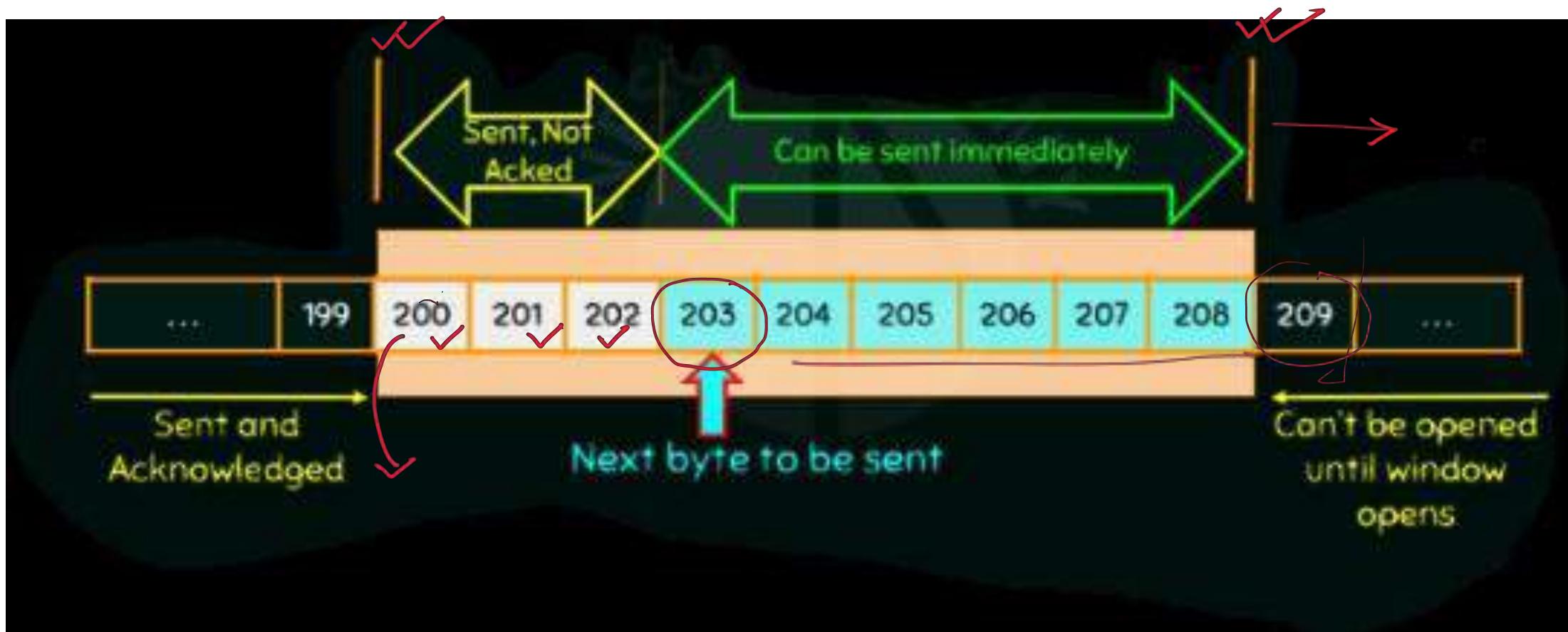
- TCP uses a sliding window to handle flow control. ✓
- Between Go-back and selective Repeat.
- Does not use NAK.
- The receiver holds out-of-order segments.
- TCP sliding window is byte-oriented. ✓
- TCP's sliding window is of variable size. ✓
- Imaginary window. ✓



TCP Sliding Window

200 kops Sender

✓ ✓
Window size = Minimum (rwnd, cwnd) = Minimum (20,9) = 9



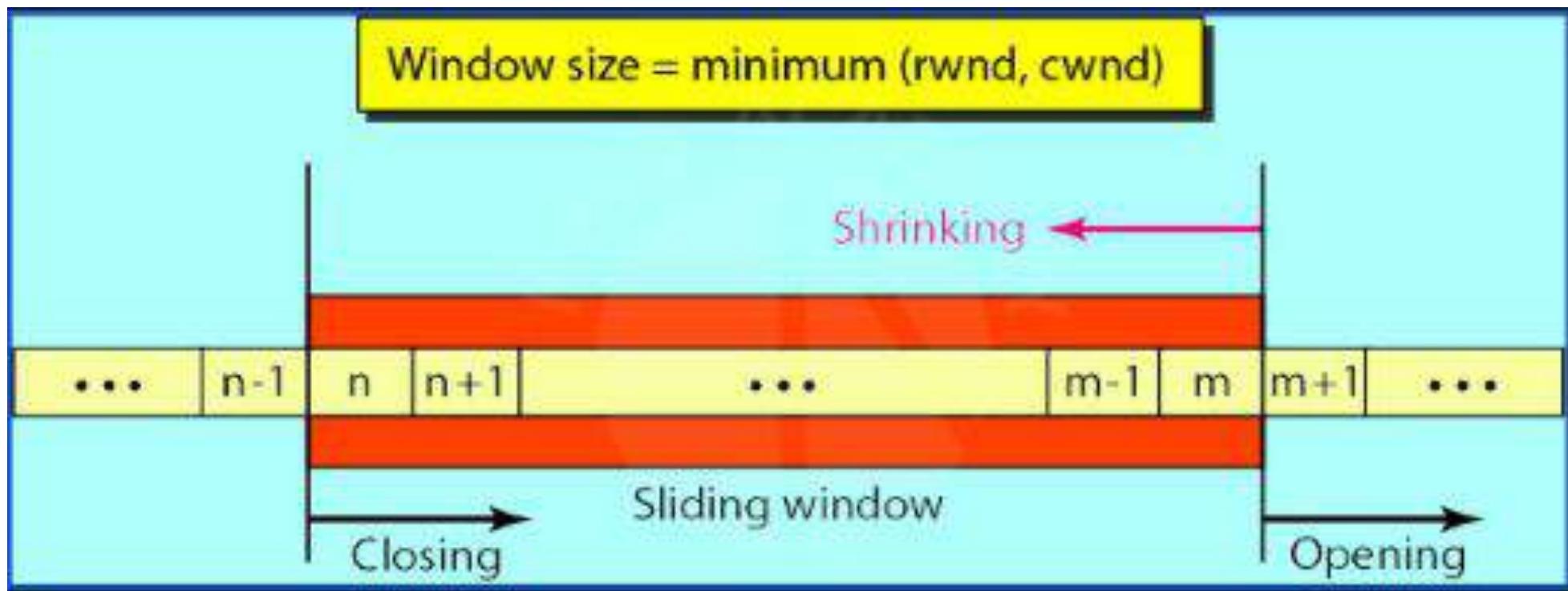
25
kb
Cw

TCP Sliding Window

Points to remember

- ◻ *Window size = Minimum (rwnd, cwnd).* ✓ ✓
- ◻ *The source does not have to send a full window's worth of data.*
- ◻ *The window can be opened or closed by the receiver, but should not be shrunk.*
- ◻ *The destination can send an ACK at any time*
- ◻ *The sender can send 1-byte segment even after the window is shut down in the receiver side.*

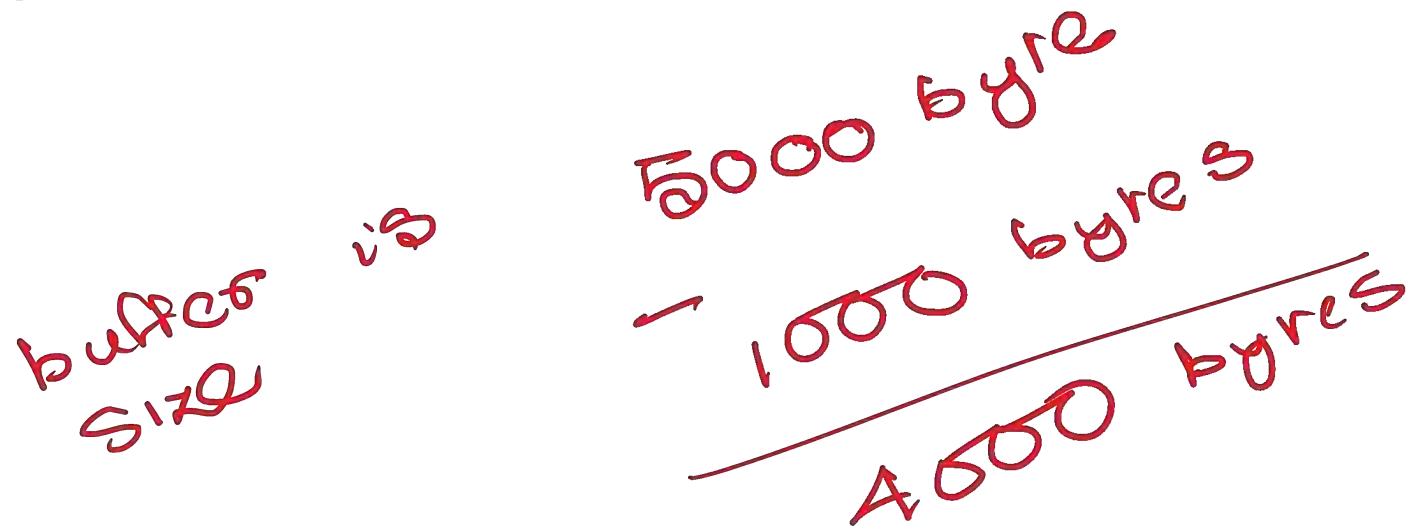
TCP Sliding Window



Questions. What is the value of the receiver window (rwnd) for host A if the receiver host B, has a buffer size of 5000 bytes and 1000 bytes of received and unprocessed data.

$$\text{Rwnd} = 5000 - 1000 = 4000 \text{ bytes}$$

Host B can only receive bytes of data before overflowing its buffer. Host B advertises this value 4000 in its next segment to Host A.



Questions. Suppose a TCP connection is transferring a file of 1000 bytes, The first byte is numbered 100001. What is the sequence number of the segment if all data is sent in only one segment?

File size = 1000 bytes

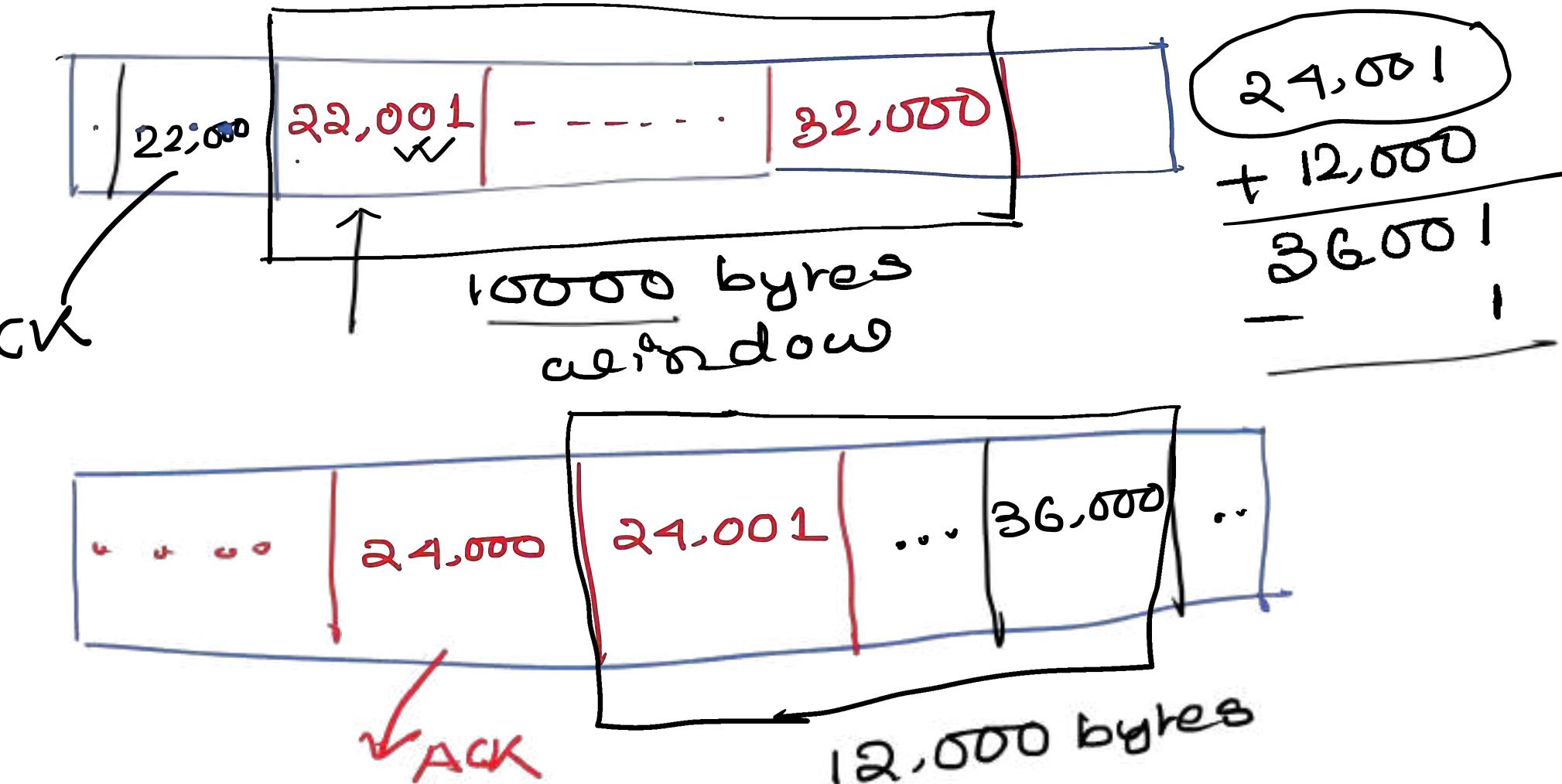
First byte of data = 10,000 + 1000

$$\begin{array}{r} 10,000 \\ + 1000 \\ \hline 10100 \end{array}$$

~~101001 bytes~~

~~101000 bytes~~

Questions. A TCP connection is using a window size of 10,000 bytes, and the previous acknowledgement number was 22,001. It receives a segment with acknowledgement number 24,001 and window size advertisement of 12,000. Draw a diagram to show the situation of the window before and after.



22,001
 + 10,000
 32,000
 -
 22,000
 36,001
 -
 successfull
 receiver
 now the
 receiver
 expect
 (22,000)

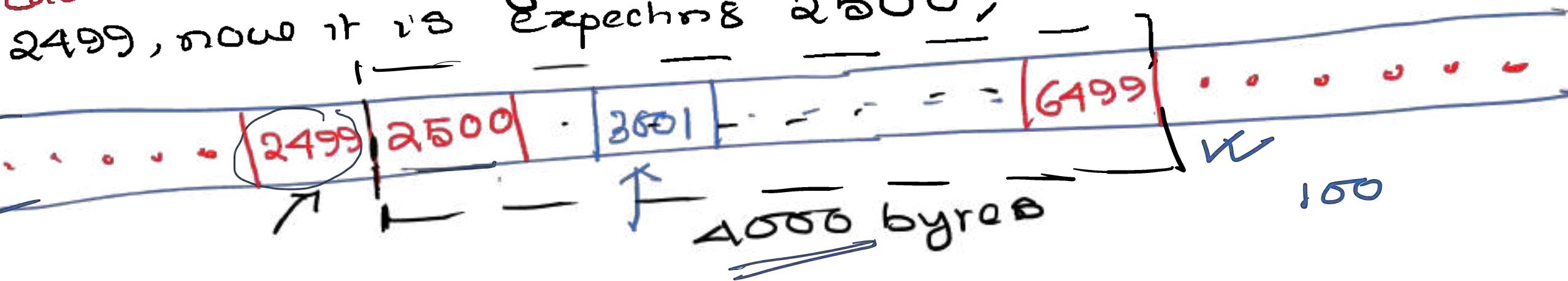
Questions. A window holds bytes 2001 to 5000. The next byte to be sent is 3001. Draw a figure to show the situation of the window after the following two events.

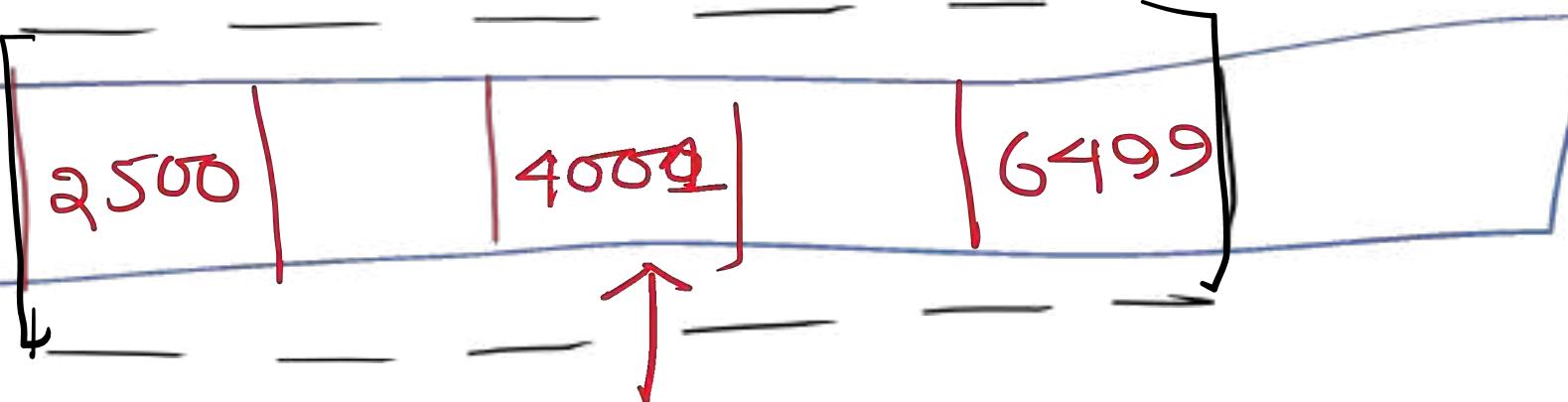
- a. An ACK segment with the acknowledgement number 2500 and window size advertisement 4000 is received. ✓

- b. A segment carrying 1000 bytes is sent. ✓



Case 1:- successfully received the segment with seq no 2499, now it's expecting 2500, window = 4000

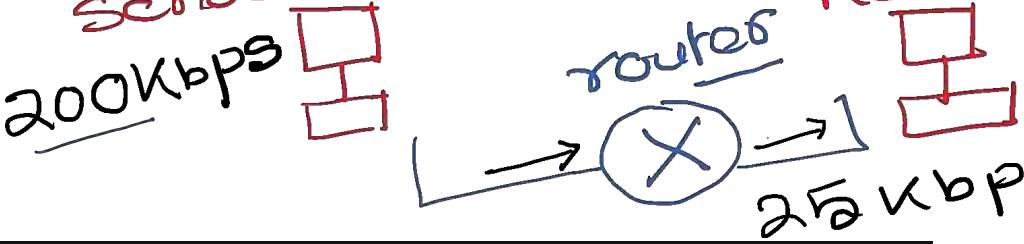




next
byte
to be sent

3001
↑
1000 bytes

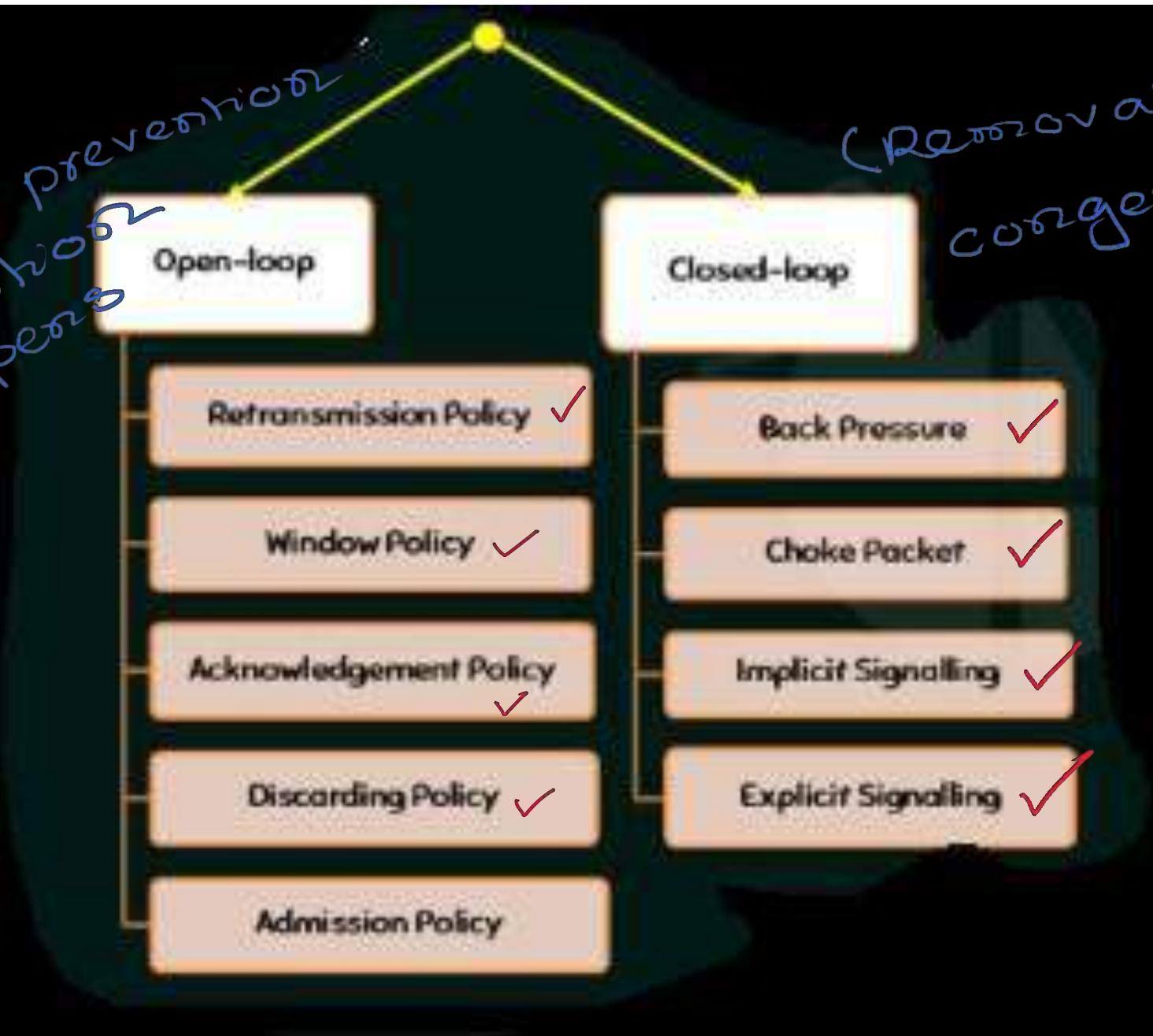
$\rightarrow \frac{30}{40}$



Congestion Control

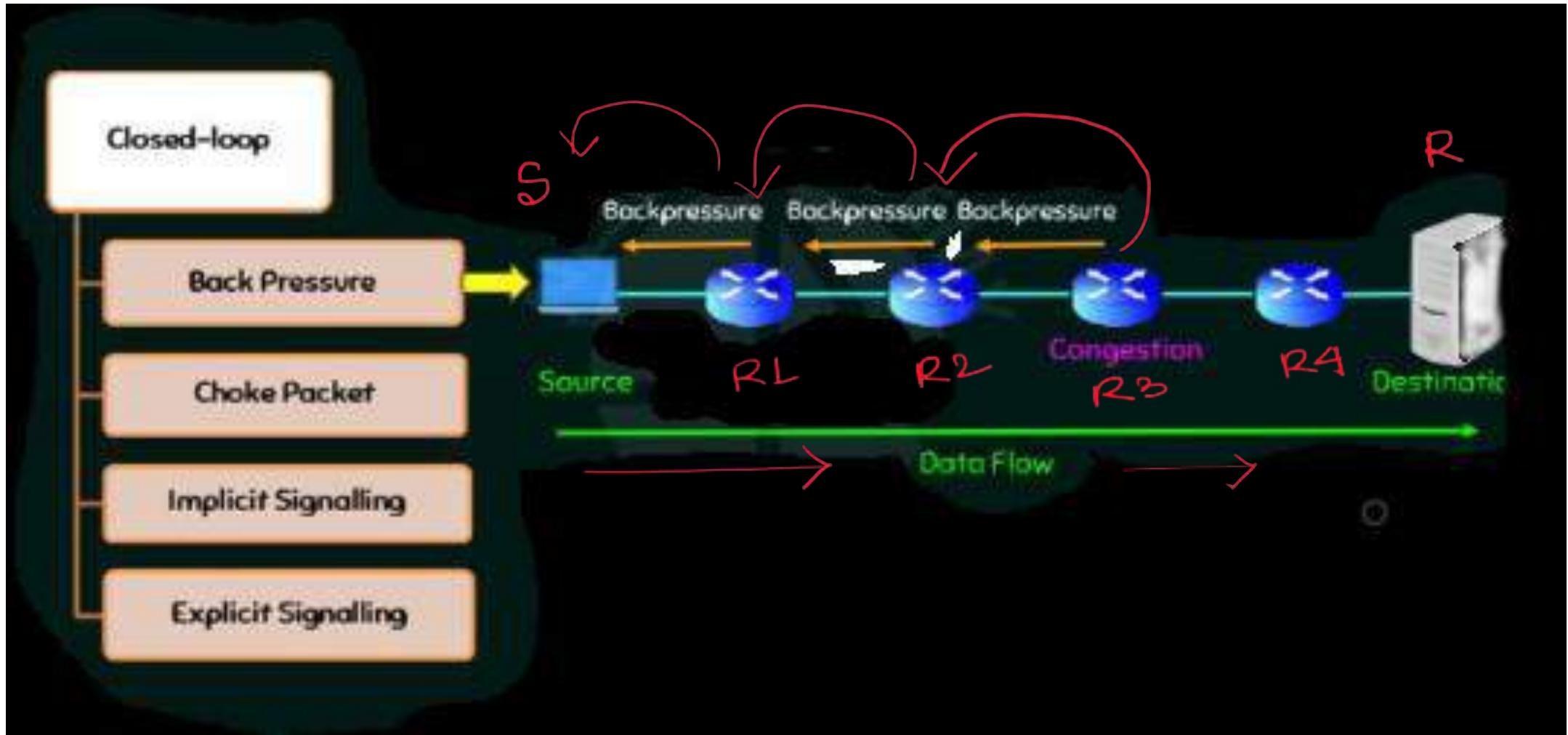


before
congestion
happens



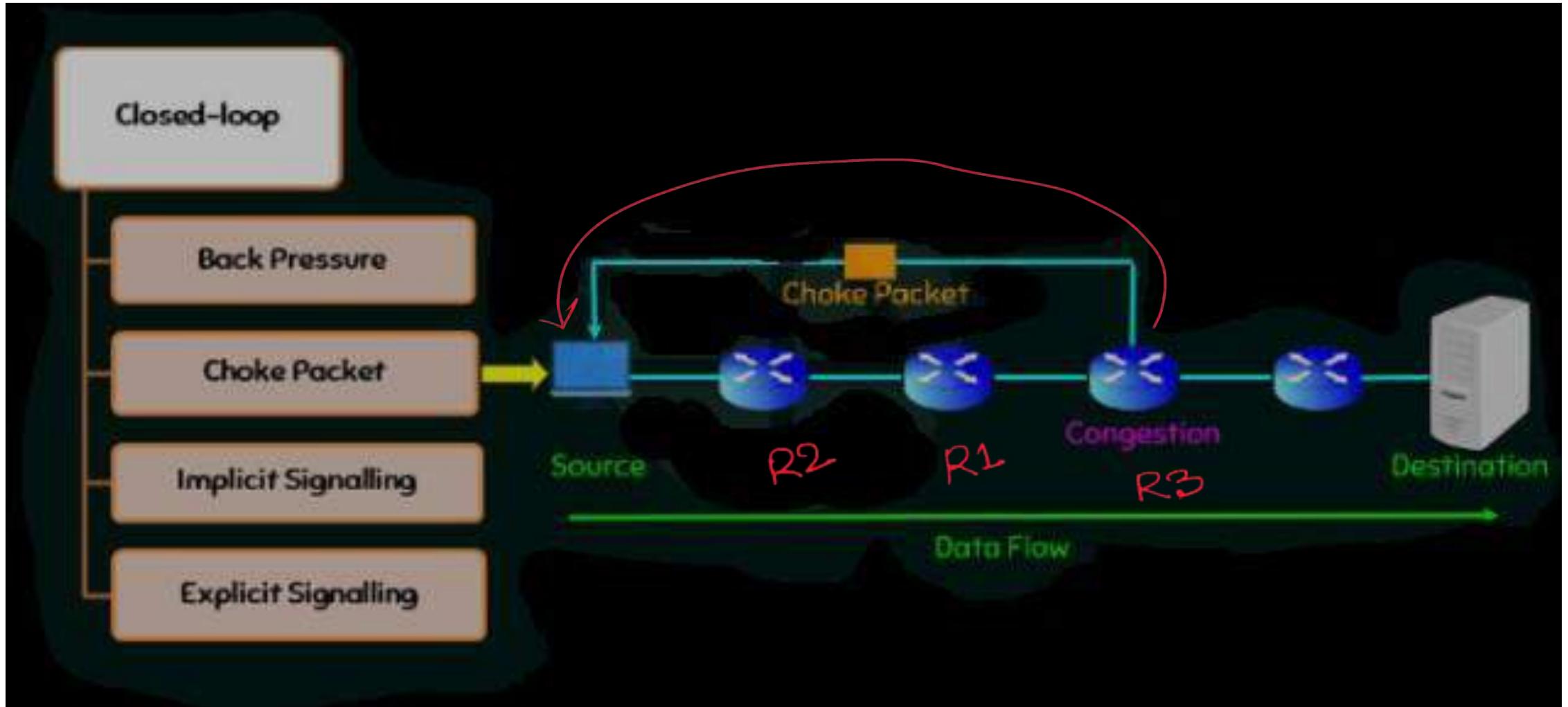
removable once the
congestion has
happened

Congestion Control

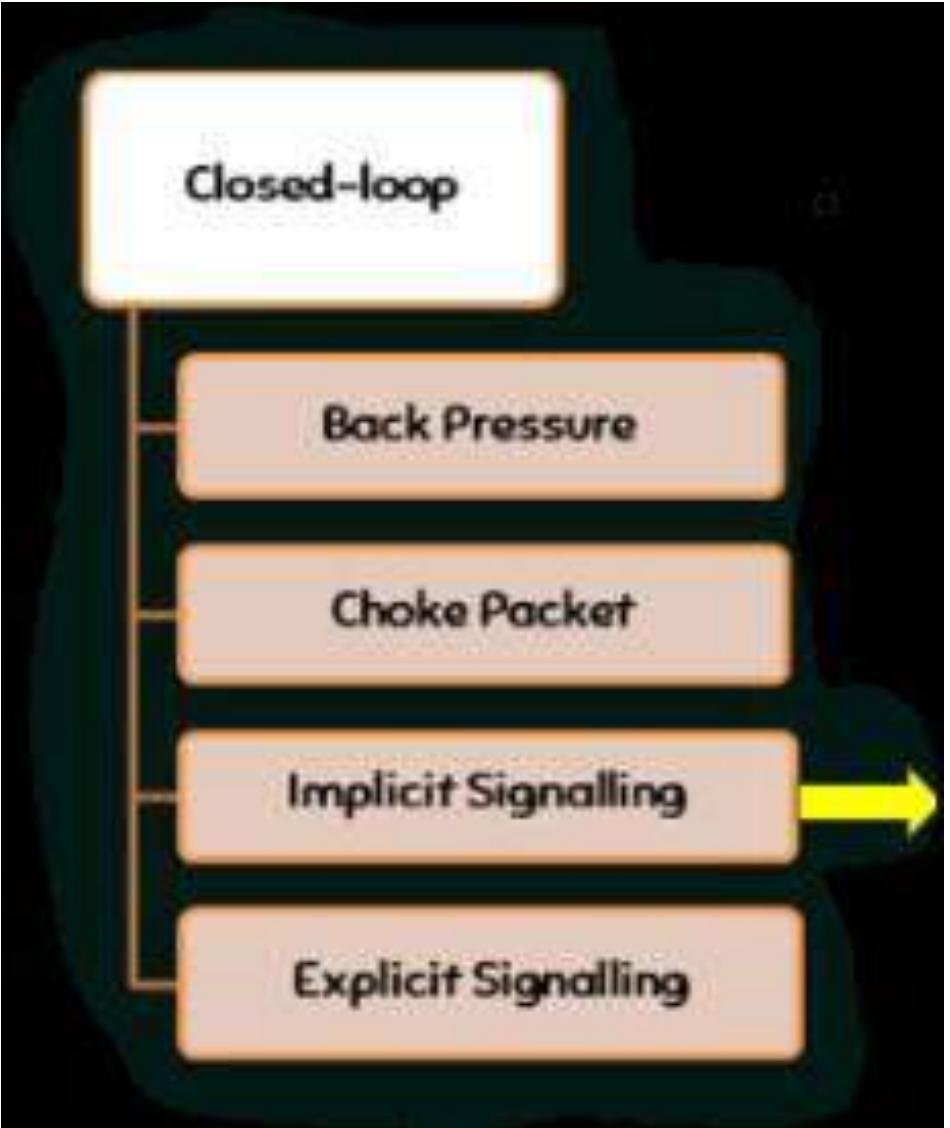


Congestion Control

ICMP

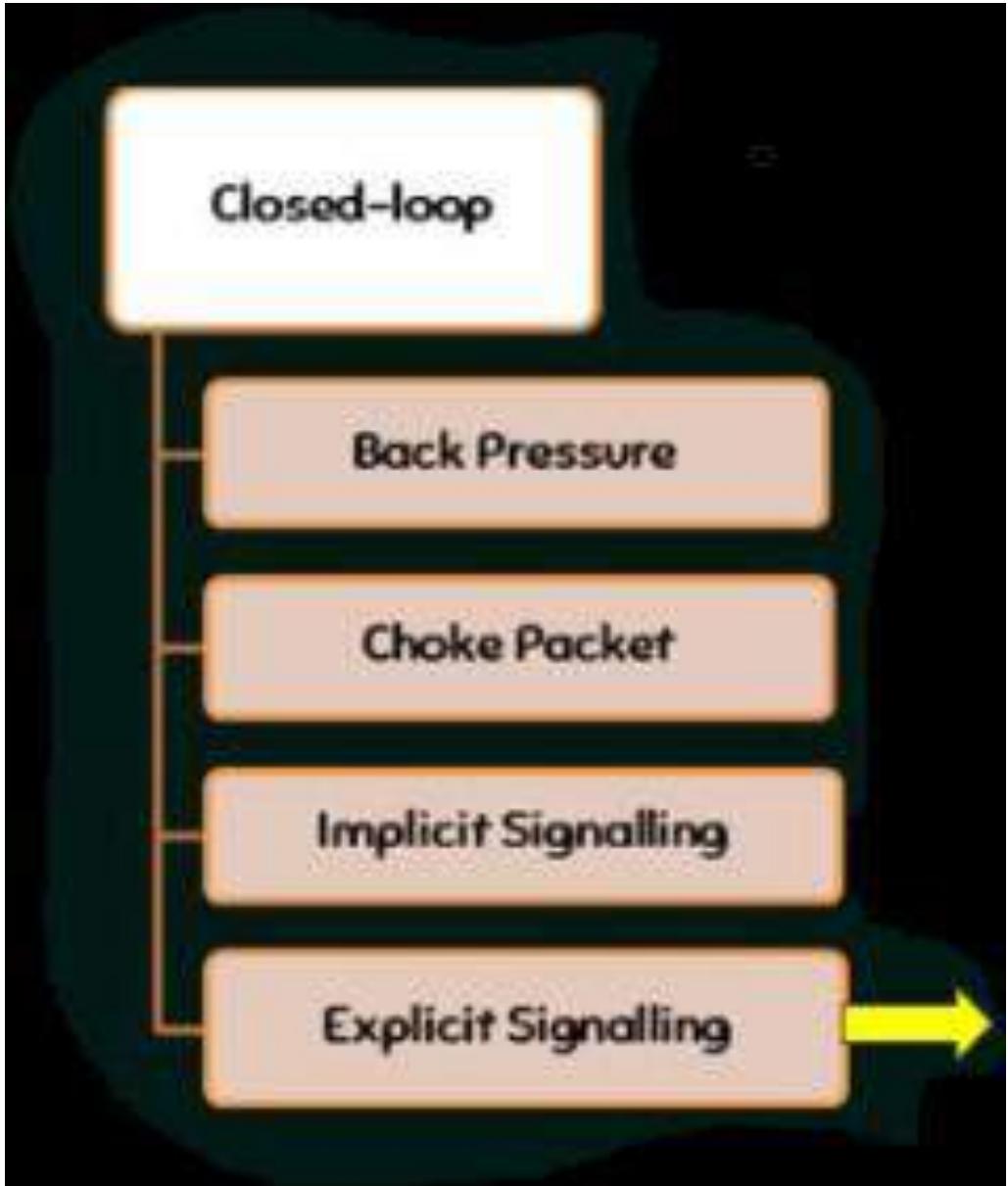


Congestion Control



- *There will be no implicit communication between the congested node and the source.*
- *The source will get to know about the congestion by no ACK packet received or delayed ACK.*

Congestion Control



- There will be explicit communication between the congested node and the source.
- Here signals will be included in the data packet itself. Router can discard less sensitive packets that carry data.

Congestion control in TCP

- The sender window size is determined by the available buffer space in the receiver (rwnd).
- In other words, we assumed that it is only the receiver that can dictate to the sender the size of the sender's window.
- If the network cannot deliver the data as fast as they are created by the sender, it must tell the sender to slow down.
- The sender's window size is determined not only by the receiver but also by congestion in the network. TCP sliding window is byte-oriented.
- Actual window size = Minimum (rwnd, cwnd)
- TCP's general policy for handling congestion is based on three phases:
 - Slow start Phase ✓ → Slow start
 - Congestion Avoidance ✓ → Additive increase
 - Congestion Detection ✓ → Multiplicative decrease

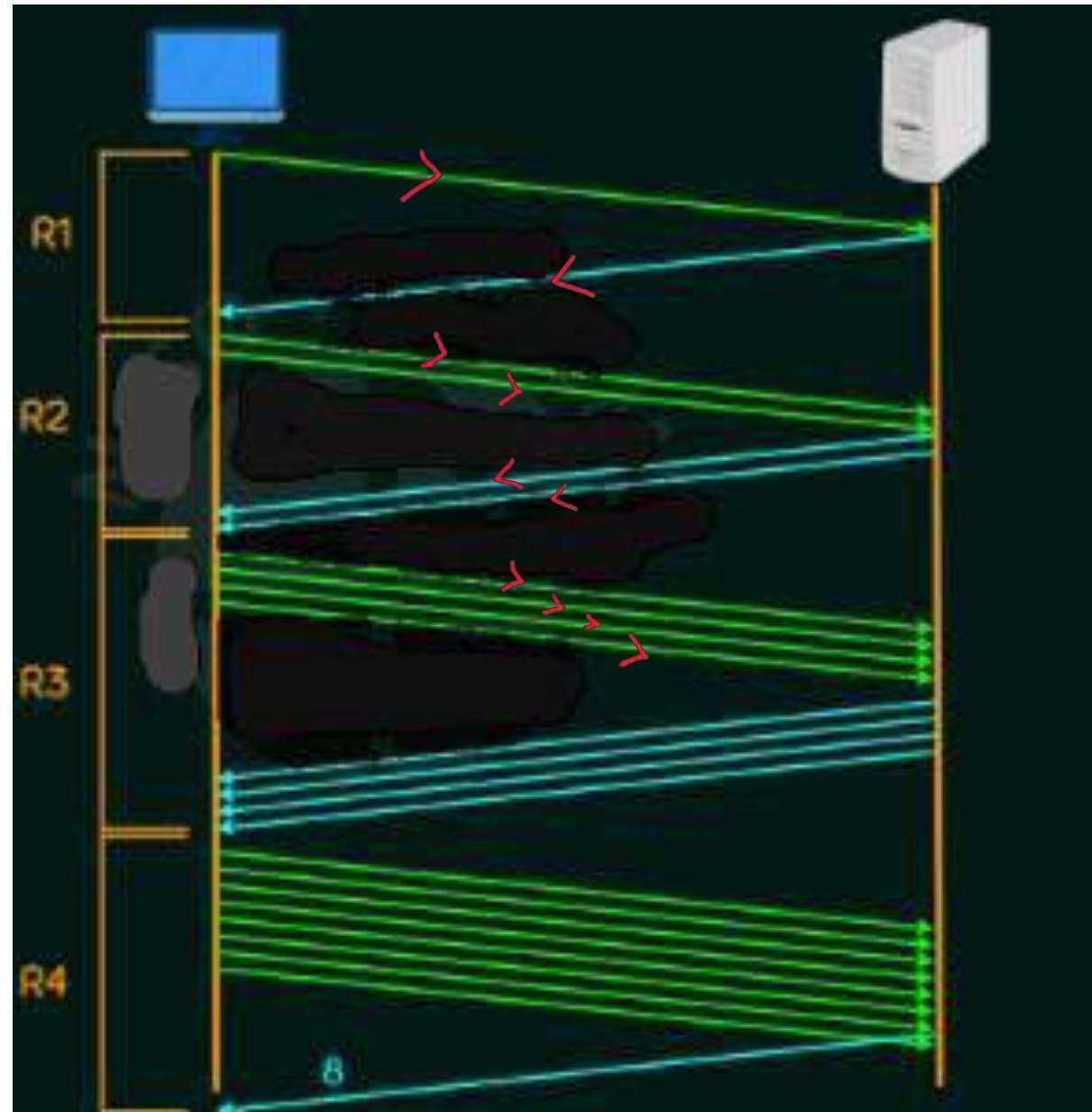
Congestion control in TCP

- In the slow-start phase, the sender starts with a very slow rate of transmission, but increase the rate rapidly to reach a threshold.
- When the threshold is reached, the data rate is reduced to avoid congestion.
- Finally congestion is detected, the sender goes back to the slow-state or congestion avoidance phase based on how the congestion is detected.

Congestion Policy

- Slow start (slow start phase)
- Additive Increase (avoid once)
- Multiplicative decrease (congestion detection)

Slow Start ✓



Round	Value of cwnd
Start	$2^0 = 1$ ✓
After Round 1	$2^1 = 2$ ✓
After Round 2	$2^2 = 4$ ✓
After Round 3	$2^3 = 8$ ✓
After Round 4	$2^4 = 16$ ✓
After Round 5	$2^5 = 32$ ✓
After Round 6	$2^6 = 64$ ✓

slow threshold

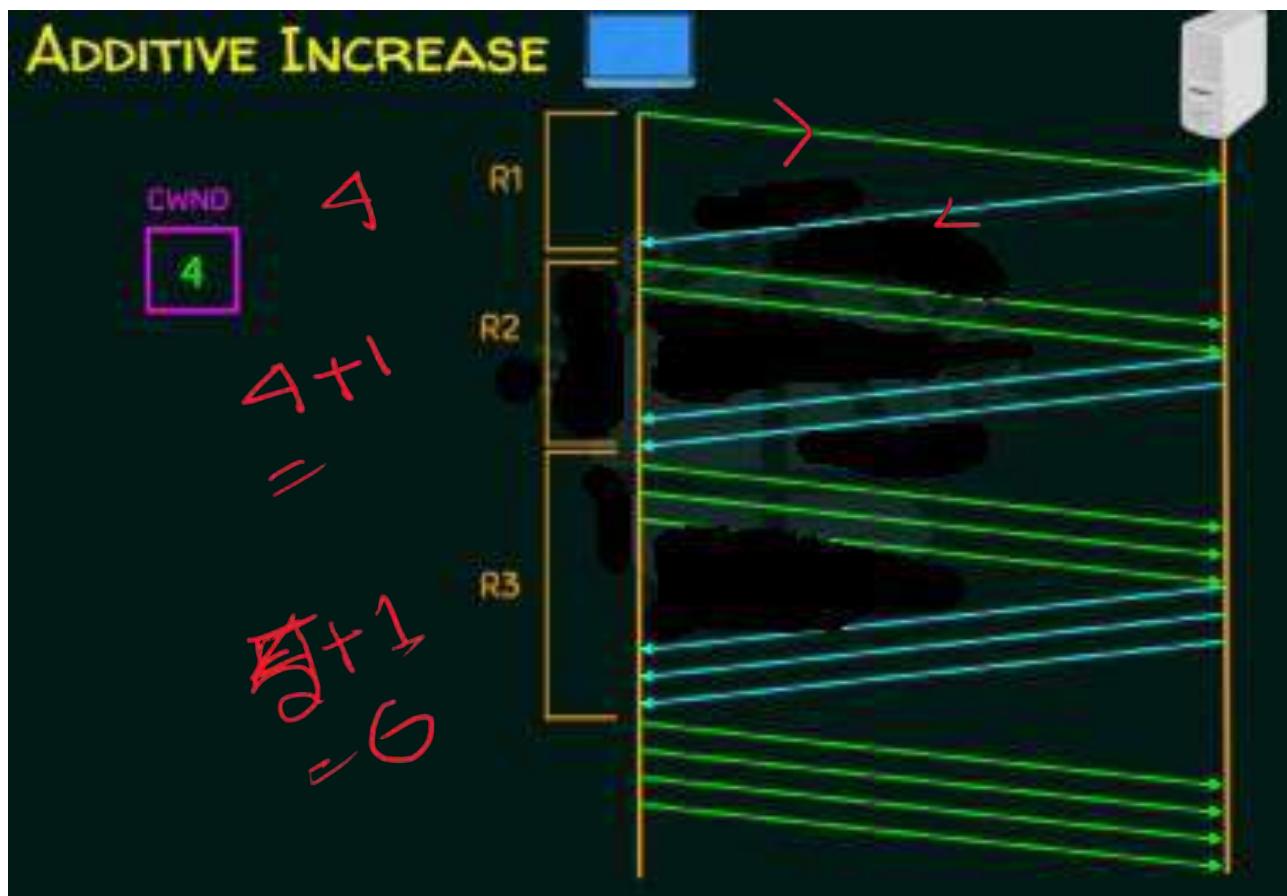
Congestion Policy

- Slow start cannot continue indefinitely.
- There must be a threshold to stop this exponential growth.
- The sender keeps track of a variable named *ssthresh* (slow-start-threshold).
- When the size of window in bytes reaches the threshold, slow start stops and the next phase starts.
- In most implementations, the value of *ssthresh* is 65,535 bytes.

Congestion Policy

- Slow start- cwnd increase exponentially.
- The exponential growth must be slowed down, to avoid congestion before it happens.
- Collision avoidance: Additive increase.
- When cwnd reaches the threshold, the slow-start phase stops and the additive phase begins.
- In this algorithm, each time the whole window of segments is acknowledged (one round), the size of the congestion window is increased by 1.
- In the congestion avoidance algorithm, the size of the congestion window increase additively until congestion is detected.

Additive Increase ✓



ADDITIVE INCREASE

Round	Value of cwnd
Start	1
After Round 1	2
After Round 2	3
After Round 3	4
After Round 4	5
After Round 5	6
After Round 6	7

Multiplicative Decrease ✓

- Slow start- Exponential increase..
- Additive increase- Linear increase.
- The cwnd must be decreased , if there is a congestion.
- Sender can guess that congestion.
- Retransmission of segment.
- Retransmission can occur in one of two cases:
 - ❖ When a timer times out or
 - ❖ When three ACKs are received.
- Threshold is dropped to one-half, a multiplicative decrease.

A hand-drawn diagram illustrating a multiplicative decrease. It shows a large circle containing the number '20'. An arrow points from this circle to a smaller circle containing '10'. Inside the smaller circle, there is a plus sign (+) above a multiplication sign (×). Below the smaller circle is the equation '10 = 10 / 2'.

Multiplicative Decrease

TCP implementations have two reactions:

Reaction 1:

- It sets the value of the threshold to one-half of the current window size.
- It sets cwnd to the size of one segment. ✓
- It starts the Slow-start phase again.

current cwnd = $\frac{1}{2} \times 50 = 25$

cwnd = $1 \times 25 = 25$

Reaction 2:

- It sets the value of the threshold to one-half of the current window size.
- It sets cwnd to the value of the threshold.
- It starts the congestion avoidance phase.

additive increase

cwnd = $25 \rightarrow +1 +1$

Multiplicative Decrease

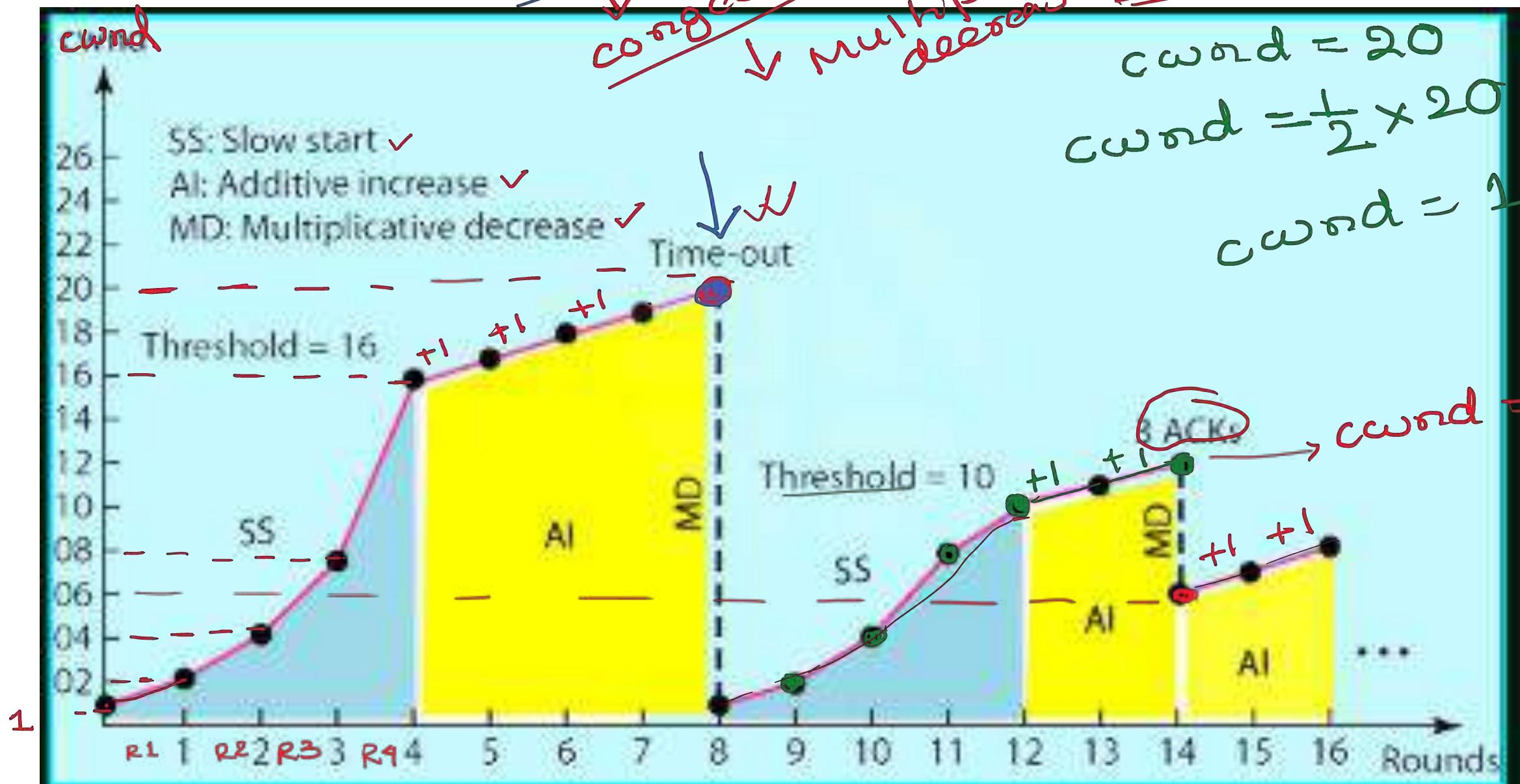
Time-out
congestion or w
multivalue
decrease 16 = ss threshold

$$cwnd = 20$$

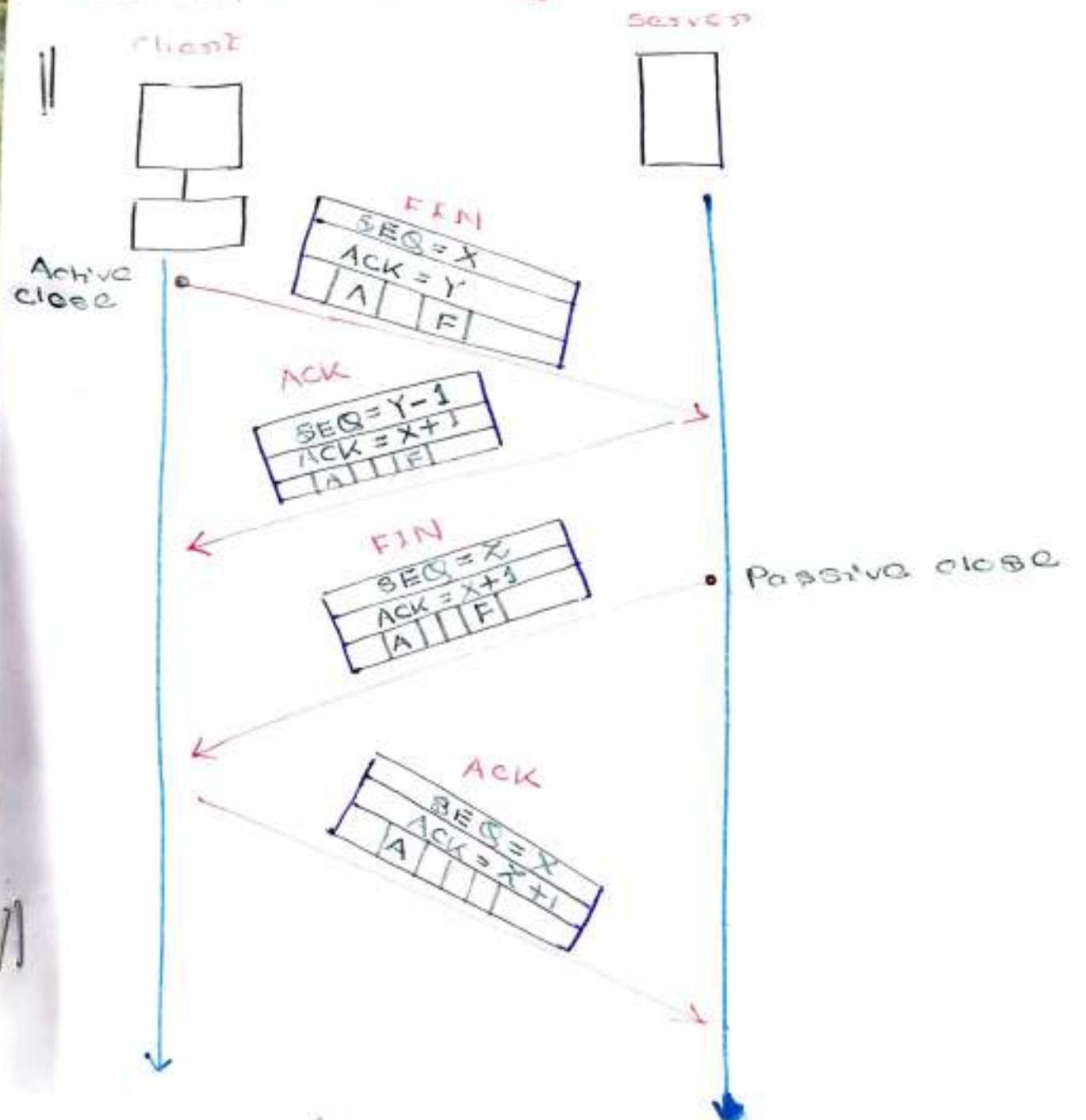
$$cwnd = \frac{1}{2} \times 20$$

$$cwnd = 1$$

cwnd
l. cong
caved



Four way handshaking :-



Sliding windows:- window is used for flow control at the receiver.
Flow control is usually done in two layers:-

1. Transport layer.

2. Data link layer.

Now we are in Transport layer:-

Now we are in Transport layer to handle flow control.

• TCP uses a sliding window to handle flow control.

• From Go-back-N

• does not use NAK.

• The receiver holds out-of-order segments

• TCP sliding window vs

• of variable size. whereas as datalink

layer sliding window vs of fixed size.

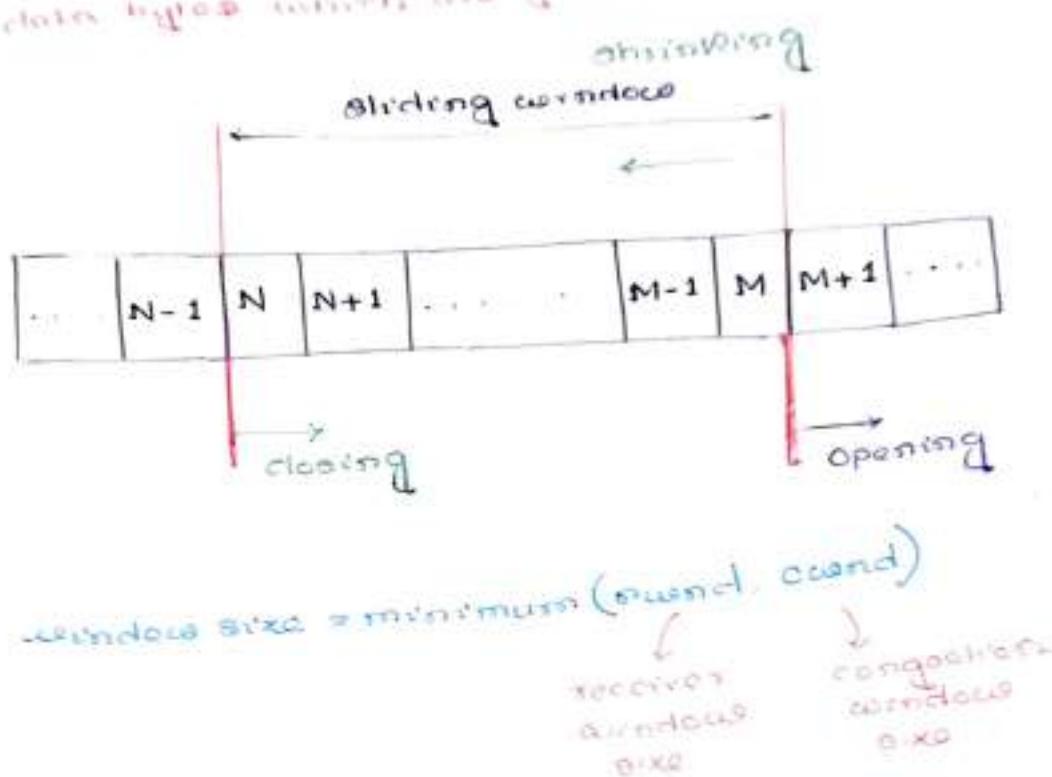
layer sliding window vs by re-oriented.

• TCP Sliding window vs by re-oriented.
whereas datalink layer sliding window vs
of frame oriented.

- the nucleus take care about

 - ④ the date input correct and good
 - ⑤ the date input correct and have check or evaluated good
 - ⑥ the date input correct and you're good

showing



The window size is of variable length.
The data which are sent but not have been
acknowledged and the data which are to be sent
immediately as will be in the window.
Suppose the N number segments sent and all
acknowledged now the window will move towards
 $(N+1)$ and now the window can allow the
 $(M+1)$ number segment to the next segment
to be sent in the queue.

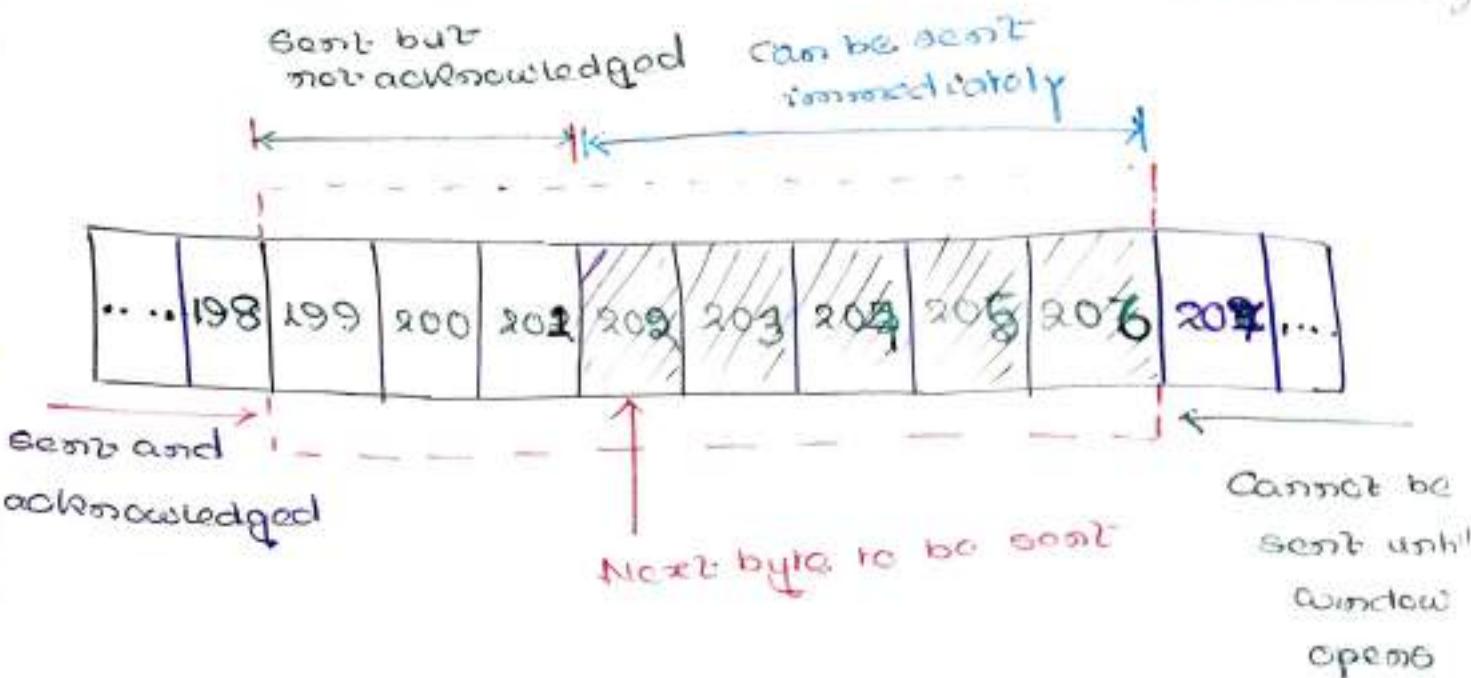
* Congestion window is the poor feature of intermediate
devices such as router or switches. suppose
the receiver has a window size of 50. But
the router through which many segments of
other ongoing communications are
processing, so there is a congestion.

$$\text{window size} = \min(\text{round}, \text{wind}) = 8$$

receive window size

congestion window size

(size of network window)



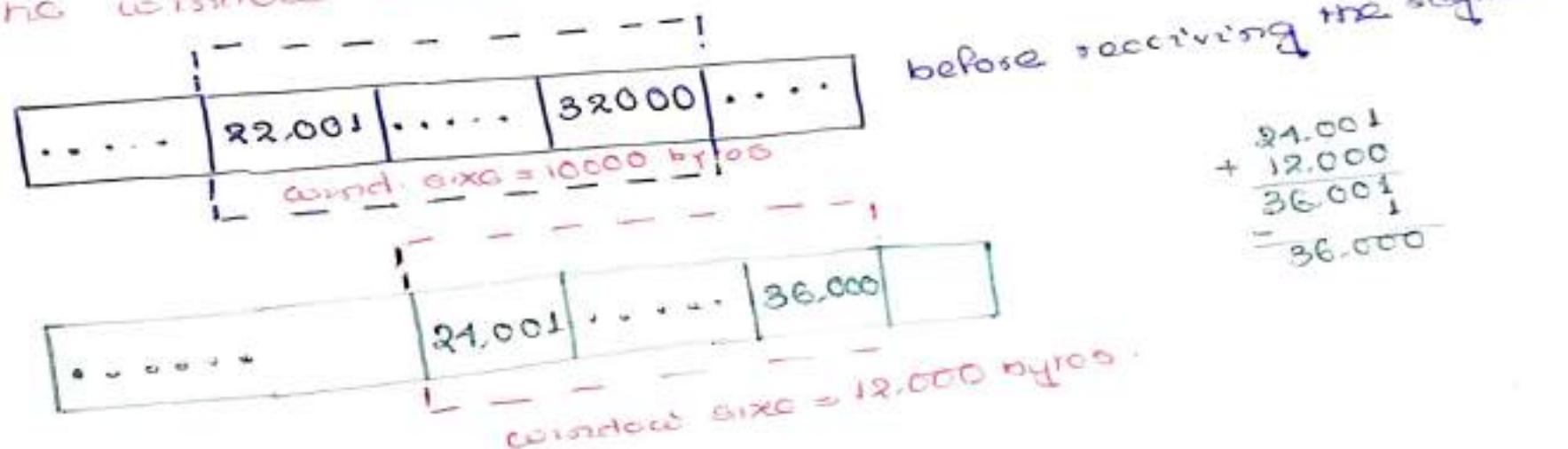
- window size $\leq \min(\text{round}, \text{wind})$.
- The source does not have to send a full window's worth of data.
- The window can be opened or closed by the receiver but should not be shrunk.
- The destination/receiver can send an ACK at any time.
- The sender can send 1-byte segment even after the window is shut down in the receiver side.

Q. what is the size of the window for host A if the value of send (receive window) is 3000 bytes and the value of cwnd (congestion window) is 3500 bytes?

$$\Rightarrow \text{we know, } \text{window size} = \min(\text{send}, \text{cwnd}) \\ = \min(3000, 3500) \\ = 3000 \text{ bytes}$$

Q. A TCP connection is using a window size of 10,000 bytes and the previous acknowledgement number was 22,001. It receives a segment with acknowledgement number 21,001 and window size advertisement of 19,000. Draw a diagram to show the situation of the window before and after.

$$\begin{array}{r} 22,001 \\ + 18,000 \\ \hline 32,001 \\ - 32,000 \\ \hline 0 \end{array}$$



Q. A window moves by 1000 bytes from 2001 to 5000.

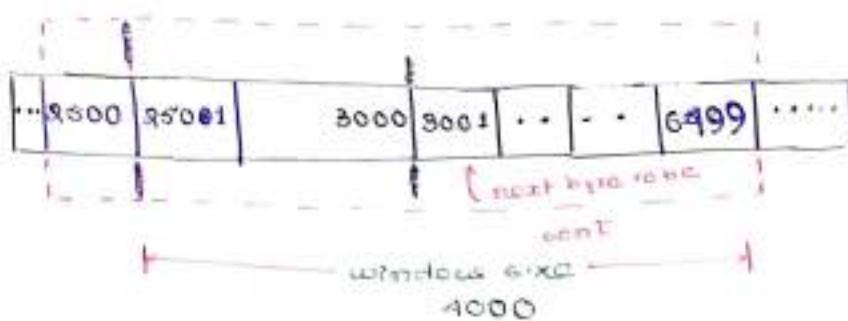
The next byte to be sent is 3001.

Draw a figure to show the situation of windows after the following two events:-
of the windows after the following two events:-

(i) An ACK segment with the acknowledgement number 2500 and window size advt. 1000 is received.

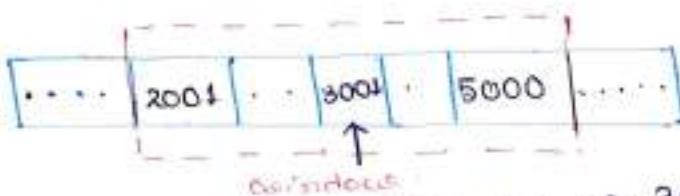
ans: 2500 and window size 1000 is received.

(ii) A segment carrying 1000 bytes is sent.



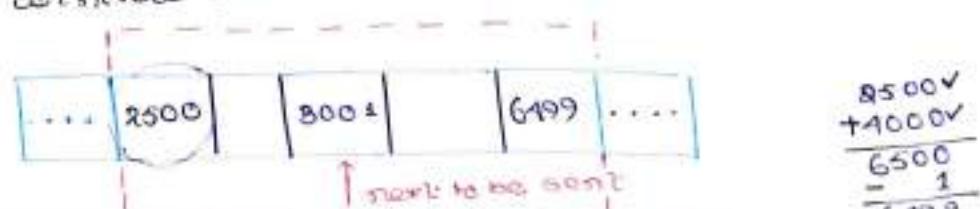
$$\begin{array}{r} 2501 \\ + 1000 \\ \hline 3501 \\ - 6500 \\ \hline 6500 \end{array}$$

Initial Figure:- The window holds bytes 2001 to 5000.

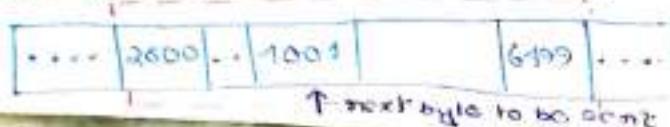


The next data byte to be sent is 3001.

An acknowledgement for 2500 is received and the new window size is 4000.



A segment carrying 1000 bytes is sent means from 3001 next 1000 bytes is sent.

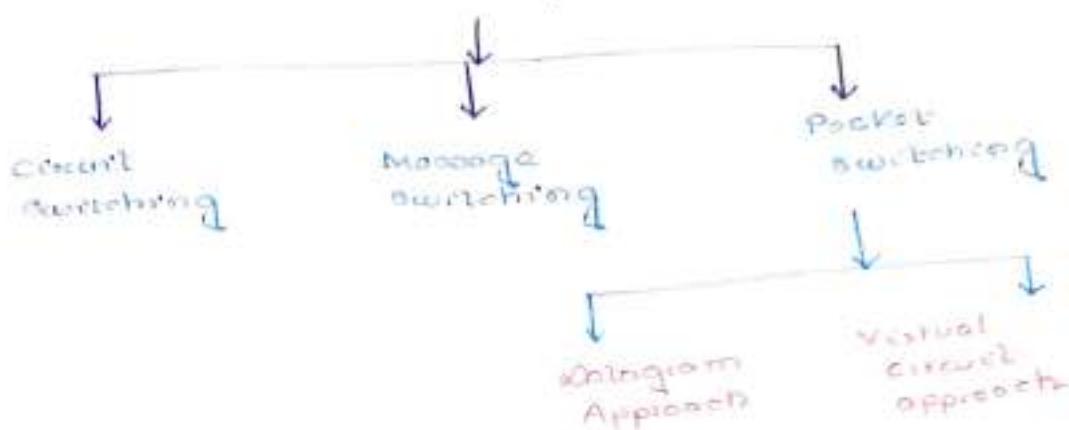


From 3001 to 4000 next 1000 bytes sent.

Switching

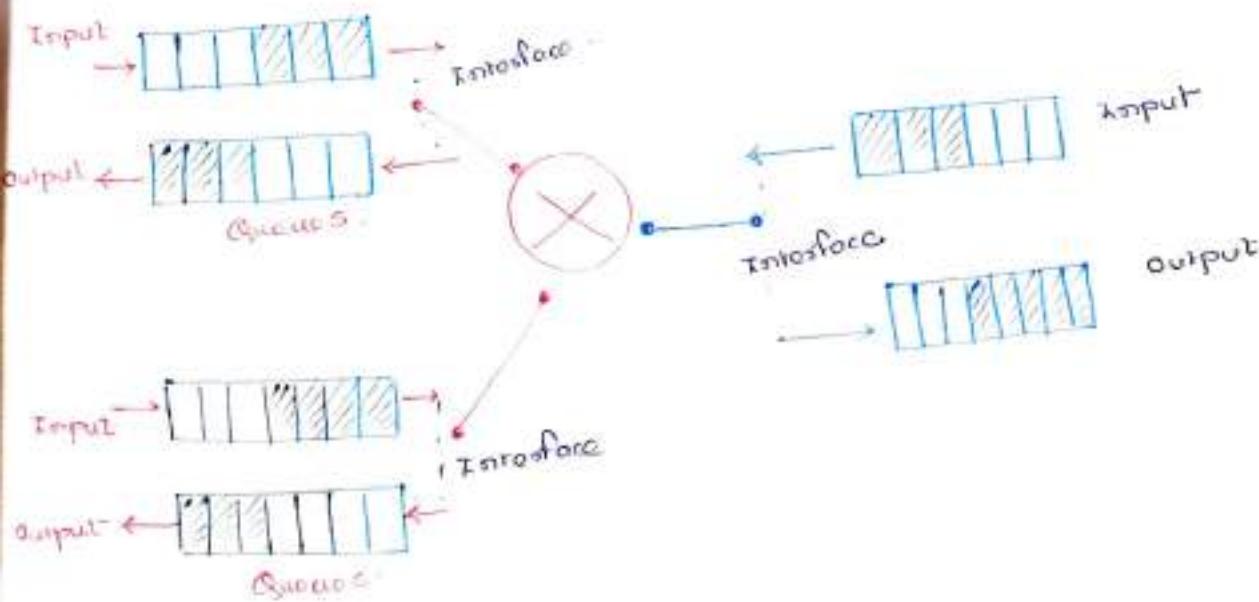
We know there are three types of switching.

Switching Techniques



Internetwork communication is not possible without routers. But router has limited memory capacity. Router has memories as form of queues.

Suppose a movie hall has limited amount of seats. As there are no prior seat booking is allowed. If the number of people arrived at the hall is large than the no. of available seats then the congestion occurs. Same way congestion in computer network occurs at the source/switches/computer as routers maintains buffering-queues before and after processing the data.



- (i) The purpose was put on the need of the system.
- (ii) Prevention of packet loss by adding the queue in the system. The queue can be added to the system to prevent fragmentation. For this the queue has to be added and buffering can be done.

- (iii) The receiver will give the feedback to the sender.

* It is the acknowledgement of the information received by the sender which is required to receive the information. So, the receiver has to send back the acknowledgement with the corresponding sequence number with which it has received the message.

Classification :-

(a)	Open-loop Supervision (transmitter control)	Closed-loop After acknowledgment Method	After transmission
→ Retransmission policy		→ Back pressure	
→ Acks loss policy		→ Choke packet	
→ ACK retransmission policy		→ Implicit signalling	
→ Discarding policy		→ Explicit signalling	
→ Admission policy			

Open-loop supervision of data transmission:-

- Retransmission policy:-
- As reliability is guaranteed in TCP so till the time acknowledgement is received by the receiver the data packets will be retransmitted.
- Retransmission will also be done because of loss or corrupted or damaged packets.
- But this will increase overhead.

- A good transmission control policy can help
- The TCP's transmission control policy is designed to prevent or alleviate congestions

Windows Policy:-

- Windows at sender may also affect congestion Suppose, in a busy or congested network, if the window size at the sender is large then sender will be sending more no. of data packets which can again make the network more congested
- SR (Selective Repeat) windowing is more better than Go-back-N window In Go-back-N if one segment is corrupted or missing or damaged then the entire window is retransmitted, whereas in selective Repeat window only the missing/corrupted segment is retransmitted again. Duplication in Go-back-N may worse
- This duplication is Go-back-N may worse
- Selective Repeat retransmits only lost or corrupted packets.

Acknowledgment Policy:-

- Ack policy imposed by the receiver may also affect congestion Suppose there are 10 (N=10) packets. If the network is already congested and adversary must has to be sent too much of the 10 packets then the network will be loaded by both data and also with acknowledgement packets. So either this sender's Ack for each individual packet or acknowledgement can be sent for N=10 packets together, which favors ACKS impose less load.

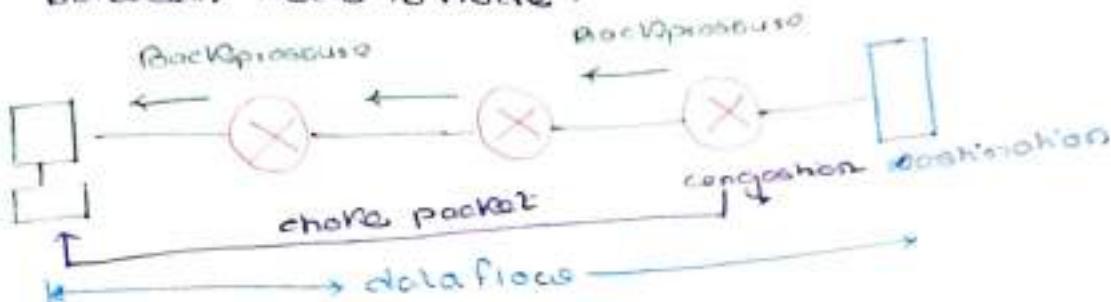
Indexable Window

- A good indexing policy can be discarded if less accurate data becomes too important than by discarding poor less important or entire data packages can have the same kind of the data some will acceptable when the type of discarding policy can move the more less compressed.
- Partitioning is another way

- Row-oriented processing provides a compact representation of data. Critical event detection is the principal application of row-oriented processing. It is used to detect changes in the environment. In the environment, objects are classified into objects which are moving and stationary. Objects which are moving are tracked and objects which are stationary are discarded.
- Space-time cube is a three-dimensional representation of data. It is used to store and retrieve data in the environment.
- Region-based processing is also called Region coding.

closed-loop Congestion control :-

→ Backpressure mechanism is a virtual connection control mechanism in node between node to node.



Cannot be applied to datagram.

Opposite direction to the dataflow.
It will inform the previous upstream node about the congestion in one node.

choke packet :-

choke packet is now a node-to-node mechanism.
choke packet is directly sent between the congested node and the source. It is a special type of packet where it will not pass through the intermediate node and will be sent directly to the source. Previous control choke packet will take help of ICMP messages.

implicit signalling :-

There will be no implicit communication between the congested node and the source to between the congested node and intermediate nodes. The source will go ~~to~~ to know about the congestion by No ACK (acknowledgment) packet received or delayed ACK.

Explicit signalling:-

There will be ~~no~~ explicit between congested node
between and source. More signals will be
included in the data packets itself.

- Routers can discard less sensitive packets
than carry data.
- There are two types of explicit signalling
 - (1) Backward signalling.
 - (2) Forward signalling.

Congestion

Congestion occurs to the input queue when the packet arrival rate is more than the processing rate of the router.

Congestion occurs at the output queue when the packet despatch rate is less than the processing rate of the router.

In both the cases there will be congestion at the router.

Who decides the window size?

$$\text{window size} = \min(\text{send window}, \text{receive window size})$$

↓ ↓
 receive window size receive window size

Each time after consulting to both the end by the sender after consulting to the intermediate devices (e.g. routers) and the receiver.

Congestion control in TCP:-

1. Slow start
2. Additive increase
3. Multiplicative decrease.

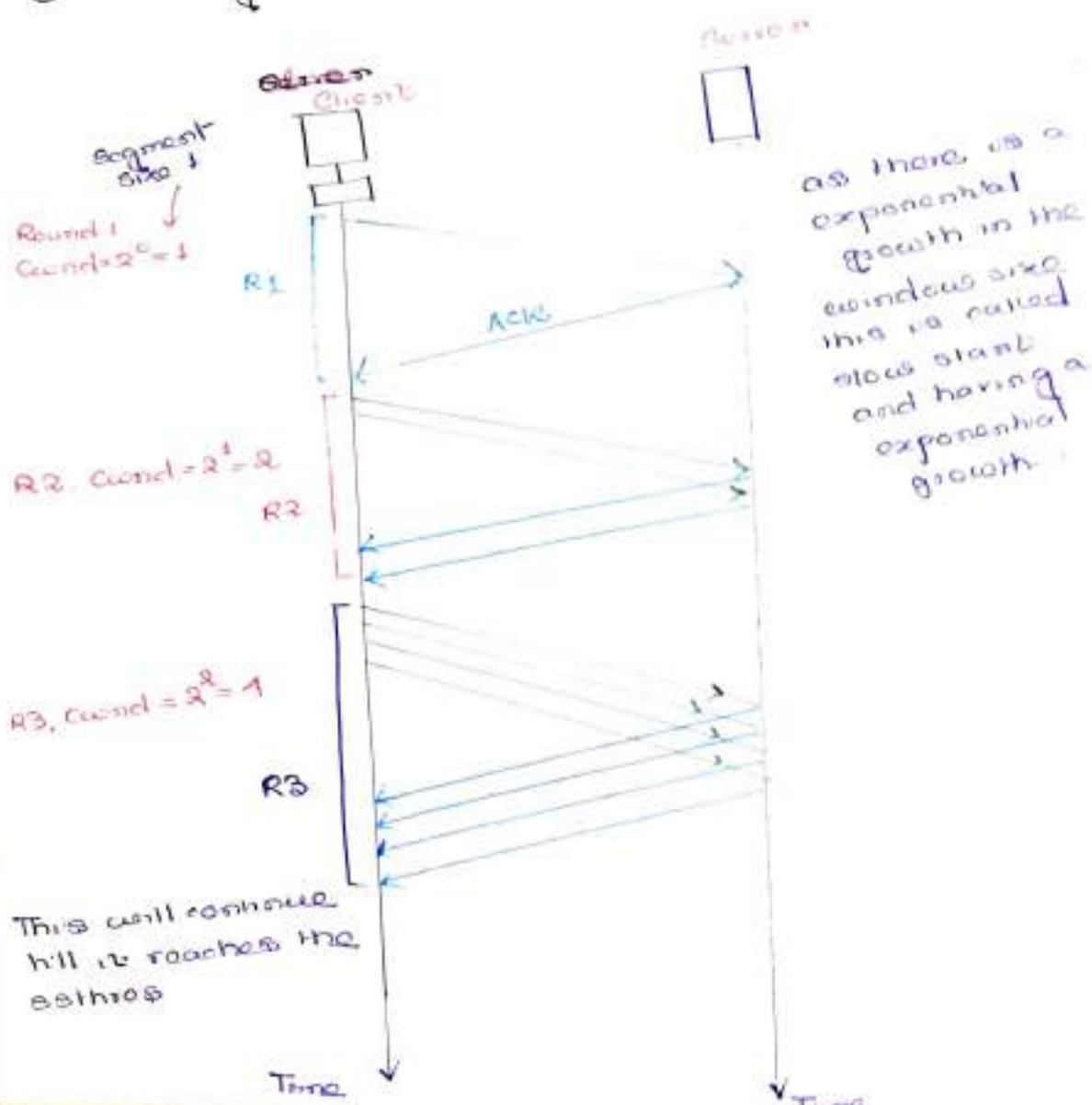
Three congestion policy

Block Start Algorithm -

- ① The size of the congestion window (round) starts with one maximum segment size (mss).
- ② The MSS is determined during TCP connection establishment.
- ③ The window starts slowly but grows exponentially.
- ④ In the block start algorithm, the size of the congestion window increases exponentially until it reaches a threshold.

Assumptions:-

- ① The value of round > round and hence the window size = round.
- ② Each segment is acknowledged individually.



1. When there is no explicit window size, it is called infinite window.
2. The sender keeps a number of windows received by the receiver (sequence numbers) until the time the receiver receives errors. It is important to know about stops and the error detection limits (Go to the Additive increase algorithm notes).
3. In most implementations, the value of w_{max} is $(2^{16}-1) \times 0.65 = 215$ bytes.

Additive Increase Algorithm -
Congestion avoidance - Additive Increase
 There are three phases in congestion control in TCP

1. slow start
2. Additive Increase (Congestion Avoidance)
3. Multiplicative Decrease (Congestion + Detection)

In slow-start process card increases exponentially in powers of 2. This exponential growth must be slowed down, to avoid congestion before it happens.

Now for congestion avoidance additive increase will be implemented. After round reaches the threshold the slow start stops and the additive phase begins.

In this algorithm, each time the whole window of segments is acknowledged (one round) the size of the congestion window is increased by 1.

Suppose in the earlier diagram (one diagram), suppose the sequence is A, i.e. after receiving the acknowledgement of round 3 v.e. R3 now the next window size will not be 2^3 (i.e. 8) it will be (2^2+1+2) i.e. 5.

In the congestion avoidance algorithm, the size of the congestion window increases additively until congestion is detected.

Common divisors - multiples of 600000 in case

~~Population growth rate = multiplication~~
Slow start - exponential increase in cases

slow start - exponential increase
additive increase - linear increase

The council must be dissolved if there is a majority - a majority is a quorum.

The round must be retransmitted.
Now sender can guess if there is a congestion
if the ack message is timed out or delayed
the segments have to be retransmitted.

If the ACK message is lost, retransmission of the segments have to occur in two cases:-

- ③ when a horse takes cur. or receives lactic ACID it is received.

- Threshold is dropped to one-half, a multiplicative decrease. when the window reaches the bottleneck (suppose the value is 20) and congestion is sensed by the sender, transmission has to be done, and then this time the ~~window~~ window size will be decreased to $(\frac{1}{2} \times 20 = 10)$

Now often retransmits occurs TCP implementers have two techniques:-

name two? _____

- now two reaches :-

Reaching 1:-

 1. It sets the value of the threshold i.e. scaled to one-half of the current window size
 2. It sets equal to the size of one segment $\Rightarrow 2^0 = 1$
 3. It starts the slow-start phase again.

3. If $\text{start} \leq \text{threshold}$ then set $\text{threshold} \rightarrow \text{one half} \text{ i.e. } \text{set} \text{ threshold} \rightarrow \text{one}$

Reaction 2 :-
the value of the threshold i.e. estimate to one
= window size.
P threshold

- Reaction 2 :-**

 1. It sets the value of the threshold half of the current window size.
 2. It sets the count to the value of threshold.
 3. It starts the congestion avoidance phase.
 4. The additive increase that is the window will be increased by 1 after each round.

[Dashboard](#) / [Courses](#) / [Autumn 2021-22](#) / [BTech Sem-5](#) / [CS301_CSE & IT](#) / [General](#)

/ [Pre-Mid-Semester Exam CS301 \(Section 1 + Section 2\)_19-08-2021 10.15 ti 11.15 AM](#)

Started on Thursday, 19 August 2021, 10:21 AM

State Finished

Completed on Thursday, 19 August 2021, 10:59 AM

Time taken 38 mins 19 secs

Grade **21.00** out of 30.00 (**70%**)

Question **1**

Complete

Mark 0.00 out of 1.00

Which is true for circuit switching?

- a. The bandwidth used is not constant.
- b. While switching, time is wasted in waiting.
- c. All of these
- d. The rate at which the data is transmitted is constant.

The correct answer is:

The rate at which the data is transmitted is constant.

Question **2**

Complete

Mark 1.00 out of 1.00

Ethernet frame consists of

- a. Default mask
- b. None of these
- c. IP address
- d. MAC address

The correct answer is:

MAC address



Question 3

Complete

Mark 1.00 out of 1.00

Which of the following is a set of rules that governs the data communication in a computer network

- a. Protocols
- b. None of these
- c. RFCs
- d. Activity standards

The correct answer is:

Protocols

Question 4

Complete

Mark 2.00 out of 2.00

What will be the propagation time when the distance between two nodes is 2400km? Assuming the communication media between the nodes is fiber cable and the light travels with a speed to be 2×10^8 m/s in the cable.

- a. 2 ms
- b. None of these
- c. 12 ms
- d. 5 ms

The correct answer is:

12 ms



Question 5

Complete

Mark 0.00 out of 2.00

A shared broadcast medium of transmission rate 5 Mbps is being shared by 10 users (U1, U2,U10). Calculate the maximum transmission rate of each of the users if the channel access scheme used is FDMA. If instead of FDMA the scheme being used is CDMA then what will be the maximum transmission rate of each of the users?

- a. 50 Mbps, 5 Mbps
- b. None of these
- c. 500 Kbps, 5000 Kbps
- d. 5000 Kbps, 5000 Kbps

The correct answer is:

500 Kbps, 5000 Kbps

Question 6

Complete

Mark 1.00 out of 1.00

A landline telephone network is an example of..... network.

- a. Circuit switched
- b. Line switched
- c. Packet switched
- d. Both packet switched and circuit switched

The correct answer is:

Circuit switched



Question 7

Complete

Mark 1.00 out of 1.00

Which sub-layer of the data link layer performs data link functions that depend upon the type of medium?

- a. Logical link control sub-layer
- b. error control sub-layer
- c. Media access control sub-layer
- d. network interface control sub-layer

The correct answer is:

Media access control sub-layer

Question 8

Complete

Mark 1.00 out of 1.00

Which address identifies a process on a host?

- a. port address
- b. physical address
- c. logical address
- d. specific address

The correct answer is:

port address



Question 9

Complete

Mark 0.00 out of 1.00

What kind of transmission medium is most appropriate to carry data in a computer network that is exposed to electrical interference?

- a. Coaxial cable
- b. Optical fiber
- c. Microwave link
- d. Un-shielded twisted pair

The correct answer is:

Optical fiber

Question 10

Complete

Mark 1.00 out of 1.00

The sharing of medium and its links by two or more devices is called

- a. Duplexing
- b. Multiplexing
- c. Fully duplexing
- d. Microplexing

The correct answer is:

Multiplexing



Question 11

Complete

Mark 1.00 out of 1.00

Transmission delay not depends upon

- a. Distance between routers
- b. Bandwidth of the medium
- c. Packet length
- d. Transmission rate

The correct answer is:

Distance between routers

Question 12

Complete

Mark 1.00 out of 1.00

In computer networks nodes are....

- a. the computer that originates/generates the data
- b. the computer that routes the data
- c. All of these
- d. the computer that terminates the data

The correct answer is:

All of these



Question 13

Complete

Mark 1.00 out of 1.00

Communication between a computer and a speaker involves

- a. Simplex
- b. Full-duplex
- c. Automatic
- d. Half-duplex

The correct answer is:

Simplex

Question 14

Complete

Mark 1.00 out of 1.00

The function of Digital Subscriber Line Access Multiplexer is to _____

- a. Amplify digital signals
- b. Convert digital signals into analog signals
- c. De-amplify digital signals
- d. Convert analog signals into digital signals

The correct answer is:

Convert analog signals into digital signals



Question 15

Complete

Mark 1.00 out of 1.00

Which of the following task is not done by data link layer?

- a. Flow control
- b. Encoding
- c. Framing
- d. Error control

The correct answer is:

Encoding

Question 16

Complete

Mark 0.00 out of 1.00

Which of the following statement is incorrect,

A shared broadcast media of transmission bandwidth 20 Mbps is shared by 100 users then,

- a. Using TDMA scheme, each of the users have an access to 200 Kbps of bandwidth
- b. Using CDMA scheme, each of the users have an access to 20 Mbps of bandwidth
- c. Using CDMA scheme, each of the users have an access to 200 Kbps of bandwidth
- d. Using FDMA scheme, each of the users have an access to 200 Kbps of bandwidth

The correct answer is:

Using CDMA scheme, each of the users have an access to 200 Kbps of bandwidth



Question 17

Complete

Mark 0.00 out of 1.00

Optical Network Terminator is connected to splitter using _____

- a. Optical cable
- b. Twisted pair cable
- c. microwave link
- d. hybrid fiber co-axial cable

The correct answer is:

Optical cable

Question 18

Complete

Mark 1.00 out of 1.00

In link layer, parity bits are used for

- a. to detect errors
- b. to identify the user
- c. encryption of data
- d. to transmit data faster

The correct answer is:

to detect errors



Question 19

Complete

Mark 1.00 out of 1.00

The number of bits in IPV4 address, IPV6 address, MAC address and Port address are

- a. 32, 128, 64, 16
- b. 128, 32, 48, 16
- c. 32, 128, 48, 32
- d. 32, 128, 48, 16

The correct answer is:

32, 128, 48, 16

Question 20

Complete

Mark 1.00 out of 1.00

Which physical media provides the highest transmission speed in a network?

- a. co-axial cable
- b. optical fiber
- c. electrical cable
- d. twisted pair cable

The correct answer is:

optical fiber



Question 21

Complete

Mark 0.00 out of 3.00

What are the propagation time and the transmission time for a 5Mbyte message (an image) if the transmission rate of the network is 1Mbps? Assume that the distance between the sender and the receiver is 8000 km and that light travels at 4×10^8 m/s.

- a. 50msecs, 40msecs
- b. 2msecs, 40msecs
- c. 2msecs, 40secs
- d. 50msecs, 40secs

The correct answer is:

2msecs, 40secs

Question 22

Complete

Mark 3.00 out of 3.00

The message 11001001 is to be transmitted using CRC polynomial x^3+1 to protect it from errors. The message that should be transmitted after appending the CRC code with the original data is

- a. 1100001010
- b. None of these
- c. 1100001011
- d. 1100001110

The correct answer is:

None of these



Question 23

Complete

Mark 1.00 out of 1.00

Which is not true for Packet switching?

- a. Installation costs of packet switching are expensive.
- b. Multiple users can use the same channel while transferring their packets.
- c. A dedicated path is followed throughout the session.
- d. The delivery of these packets becomes easy when complicated protocols are used.

The correct answer is:

A dedicated path is followed throughout the session.

Question 24

Complete

Mark 1.00 out of 1.00

Header of a frame generally contains

- a. All of these
- b. MAC addresses
- c. Synchronization bytes
- d. Frame identifier

The correct answer is:

All of these

[◀ Mid-Semester Exam_CS301 \(Section 1 + Section 2\)_13-09-2021_9.00 AM to 9.40 AM](#)

Jump to...

[Continuous LAB Assessment_24.08.2021_4.15pm to 4.30pm ►](#)

Started on Friday, 12 November 2021, 1:20 PM

State Finished

Completed on Friday, 12 November 2021, 1:28 PM

Time taken 8 mins 30 secs

Grade 7.00 out of 10.00 (70%)

Question 1

Complete

Mark 1.00 out of 1.00

The well-known port addresses are assigned to the

- a. None of these
- b. Destination
- c. Source
- d. Routers

Question 2

Complete

Mark 1.00 out of 1.00

Which fields helps to check rearrangement of the fragments in IPV4?

- a. Protocol field value
- b. Checksum
- c. Fragment Offset
- d. Flags

Question 3

Complete

Mark 1.00 out of 1.00

A email service uses which one of the following transport layer protocol?

- a. UDP
- b. Both TCP and UDP
- c. HTTP
- d. TCP

Question 4

Complete

Mark 1.00 out of 1.00

The traffic field of IPV6 is similar to which field in the IPV4 header?

- a. Fragmentation field
- b. Type of service
- c. Option field
- d. Fast switching

Question 5

Complete

Mark 1.00 out of 1.00

Fragmentation is done in layer.

- a. Transport Layer
- b. Data link Layer
- c. Physical layer
- d. Network Layer

Question 6

Complete

Mark 1.00 out of 1.00

Which of these is not a type of error-reporting message?

- a. Destination unreachable
- b. Router error
- c. Source quench
- d. Time exceeded

Question 7

Complete

Mark 0.00 out of 1.00

Which of the following is incorrect about Network Address Translation?

- a. Router will do NAT translation without configuration.
- b. NAT is a process in which one or more local IP address is translated into one or more Global IP address and vice versa.
- c. Certain application will not function while NAT is enabled.
- d. NAT results in switching path delays.

Question 8

Complete

Mark 0.00 out of 1.00

Routing inside a single administrative domain is called as..... routing.

- a. Path Vector
- b. Intra-domain
- c. Inter-domain
- d. None of these

Question 9

Complete

Mark 0.00 out of 1.00

In an IPV4 packet, the value of HLEN is 1010 in binary. How many bytes of options are being carried by this packet?

- a. 20 bytes
- b. 12 bytes
- c. 10 bytes
- d. 32 bytes

Question 10

Complete

Mark 1.00 out of 1.00

Which of the following is true for Address Resolution Protocol (ARP)?

- a. ARP request is broadcast and ARP reply is also broadcast.
- b. ARP request is broadcast and ARP reply is unicast.
- c. ARP request is unicast and ARP reply is also unicast.
- d. ARP request is unicast and ARP reply is broadcast.

Jump to...

Continuous LAB Assessment_28.10.2021_4.15pm to 4.30pm ►

Started on Tuesday, 24 August 2021, 4:19 PM

State Finished

Completed on Tuesday, 24 August 2021, 4:25 PM

Time taken 6 mins

Grade 8.00 out of 10.00 (80%)

Question 1

Complete

Mark 1.00 out of 1.00

What will be the propagation time when the distance between two points is 2400km? Assuming the propagation speed to be 4×10^8 m/s in cable

- a. 2ms
- b. 5ms
- c. 1ms
- d. 6ms

The correct answer is:

6ms

Question 2

Complete

Mark 1.00 out of 1.00

The _____ layer links network/user support layers by segmenting and rearranging the data.

- a. application layer
- b. transport layer
- c. session Layer
- d. network layer

The correct answer is:

transport layer

Question 3

Complete

Mark 0.00 out of 1.00

The OSI model was developed ____ TCP/IP model.

- a. None of these
- b. after
- c. simultaneous to
- d. prior to

The correct answer is:

after

Question 4

Complete

Mark 1.00 out of 1.00

Which multiple access techniques is used by IEEE 802.11 standards for wireless LANs?

- a. CSMA
- b. CSMA/CA
- c. ALOHA
- d. CSMA/CD

The correct answer is:

CSMA/CA

Question 5

Complete

Mark 1.00 out of 1.00

In reference to OSI model, TCP/IP model does not have ____

- a. application layer
- b. transport layer
- c. session layer
- d. application layer

The correct answer is:

session layer

Question 6

Complete

Mark 1.00 out of 1.00

Which of the following option is correct?

In wireless distribution system

- a. only one access point exists
- b. access points are not required
- c. multiple access points are inter-connected with each other
- d. there is no access point

The correct answer is:

multiple access points are inter-connected with each other

Question 7

Complete

Mark 1.00 out of 1.00

Which layer is responsible for the process to process delivery in a general network model?

- a. transport layer
- b. network layer
- c. session layer
- d. data link layer

The correct answer is:

transport layer

Question 8

Complete

Mark 1.00 out of 1.00

Transmission data rate is decided by _____

- a. network layer
- b. data link layer
- c. physical layer
- d. transport layer

The correct answer is:

physical layer

Question 9

Complete

Mark 1.00 out of 1.00

There are n stations in a slotted LAN. Each station attempts to transmit with a probability p in each time slot. What is the probability that only one station transmits in a given time slot?

- a. $1-(1-p)^{(n-1)}$
- b. $(1-p)^{(n-1)}$
- c. $p(1-p)^{(n-1)}$
- d. $np(1-p)^{(n-1)}$

The correct answer is:

$np(1-p)^{(n-1)}$

Question 10

Complete

Mark 0.00 out of 1.00

Which multiple access techniques is used by Ethernet standards for wireless LANs

- a. CSMA
- b. CSMA/CD
- c. ALOHA
- d. CSMA/CA

The correct answer is:

CSMA/CD

[◀ Pre-Mid-Semester Exam_CS301 \(Section 1 + Section 2\)_19-08-2021_10.15 ti 11.15 AM](#)[Jump to...](#)

Started on Thursday, 28 October 2021, 4:21 PM

State Finished

Completed on Thursday, 28 October 2021, 4:28 PM

Time taken 7 mins 19 secs

Grade 8.00 out of 10.00 (80%)

Question 1

Complete

Mark 1.00 out of 1.00

Which one of the following is not a function of network layer?

- a. routing
- b. congestion control
- c. error control
- d. inter-networking

Question 2

Complete

Mark 0.00 out of 1.00

For a given subnet mask 255.128.0.0, what is the number of subnets?

- a. 8
- b. 2
- c. 4
- d. 6

Question 3

Complete

Mark 1.00 out of 1.00

In a given subnet mask 255.0.0.0, what is the number of Host ID bits?

- a. 21
- b. 24
- c. 12
- d. 221

Question 4

Complete

Mark 1.00 out of 1.00

In class C classful IPv4 addressing format, the number of networks allowed under Class C addresses is

- a. 2^{24}
- b. 2^7
- c. 2^{14}
- d. 2^{21}

Question 5

Complete

Mark 1.00 out of 1.00

Error control is responsibility of which OSI layers

- a. Network and Transport layer
- b. Physical and Data link layer
- c. All of these
- d. Data link and Transport layer

Question 6

Complete

Mark 1.00 out of 1.00

Which one of the following protocol is NOT used to resolve one form of address to another one?

- a. **DNS**
- b. **ARP**
- c. **RARP**
- d. **DHCP**

Question 7

Complete

Mark 1.00 out of 1.00

While configuring the router, the IP address assigned to one port is 201.14.2.1/23. LAN1 is attached to this port of the router. Which of the following IP addresses are valid on this LAN1 interface,

- I1: 201.14.1.100**
- I2: 201.14.1.3**
- I3: 201.14.2.2**
- I4: 201.14.3.0**

- a. Only I2 and I3
- b. Only I1 and I2
- c. Only I3 and I4
- d. Only I1 and I3

Question 8

Complete

Mark 0.00 out of 1.00

Find out the invalid subnet mask from the following

- a. **223.0.0.0**
- b. **None of these**
- c. **255.255.255.252**
- d. **255.240.0.0**

Question 9

Complete

Mark 1.00 out of 1.00

In the even parity, find the parity bit of data 1001001001.

- a. **1**
- b. **X**
- c. **0**
- d. **None of these**

Question 10

Complete

Mark 1.00 out of 1.00

In the IPV4 addressing format, the number of hosts allowed under Class A addresses

- a. **2^{32-2}**
- b. **2^{24-2}**
- c. **2^{16-2}**
- d. **2^{8-2}**

[◀ Continuous Assessment_12.11.2021_1.15pm to 1.30pm](#)

Jump to...

[Announcements ►](#)

Started on Tuesday, 6 September 2022, 2:02 PM

State Finished

Completed on Tuesday, 6 September 2022, 2:41 PM

Time taken 39 mins 41 secs

Grade **22.00** out of 37.00 (59%)

Question **1**

Complete

Mark 2.00 out of 2.00

Consider the Go-back-N protocol with a sender's window size of '8'. Suppose at time 't' the next frame in the buffer (i.e. the next inorder frame) the receiver is expecting has a sequence No. 5. Assume that the medium does not reorder the messages. What is the possible set of sequence number inside the sender's window at time 't'. Assume the sender has already received acknowledgment for all the previously transmitted frames.

- a. [4, 12]
- b. None of these
- c. [5, 12]
- d. [5, 13]

The correct answer is:

[5, 12]

Question **2**

Complete

Mark 1.00 out of 1.00

In Carrier Sense Multiple Access, which CSMA scheme senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally as soon as the channel gets idle.

- a. O-persistent
- b. 1-persistent
- c. P-persistent
- d. Non-persistent

The correct answer is:

1-persistent

Question **3**

Complete

Mark 0.00 out of 1.00

Layer that translates between physical (MAC) and logical addresses is

- a. Datalink
- b. Physical
- c. Network
- d. Transport

The correct answer is:

Network

Question **4**

Complete

Mark 1.00 out of 1.00

What are not the responsibilities of the Data link Layer?

- a. Error detection
- b. Framing
- c. IP addressing
- d. MAC addressing

The correct answer is:

IP addressing

Question 5

Complete

Mark 1.00 out of 1.00

A sender-receiver employs even parity for error correction scheme, what will be the parity bit for 1001011?

- a. 1
- b. None of these
- c. 2
- d. 0

The correct answer is:

0

Question 6

Complete

Mark 0.00 out of 1.00

In the transfer of files between four pairs of client-servers through a common transmission channel of transmission rate 1 Mbps. All the server access links have a transmission rate of 2 Mbps and all the client access links have a transmission rate of 2.5 Mbps, the throughput of this network will be

- a. 0.25 Mbps
- b. 2 Mbps
- c. 2.5 Mbps
- d. None of these

The correct answer is:

0.25 Mbps

Question 7

Complete

Mark 1.00 out of 1.00

Which is not true for Packet switching?

- a. Multiple users can use the same channel while transferring their packets.
- b. Installation costs of packet switching are expensive.
- c. The delivery of these packets becomes easy when complicated protocols are used.
- d. Multiple users can use the same channel while transferring their packets.

The correct answer is:

Multiple users can use the same channel while transferring their packets.

Question 8

Complete

Mark 1.00 out of 1.00

Error detection and correction are offered by both

- a. Network Layer and Transport Layer
- b. Data link layer and Transport Layer
- c. Data link layer and Network Layer
- d. Physical Layer and Data link Layer

The correct answer is:

Data link layer and Transport Layer

Question **9**

Complete

Mark 1.00 out of 1.00

What will be the propagation time when the distance between two points is 2400km? Assuming the propagation speed to be 4×10^8 m/s in cable.

- a. 1 ms
- b. 5ms
- c. 6ms
- d. 2 ms

The correct answer is:

6ms

Question **10**

Complete

Mark 0.00 out of 1.00

Which are end system devices

- a. web servers
- b. All of these
- c. mail servers
- d. smartphones

The correct answer is:

All of these

Question 11

Complete

Mark 1.00 out of 1.00

The OSI model was developed ____ TCP/IP model.

- a. simultaneous to
- b. prior to
- c. after
- d. with no link to TCP/IP

The correct answer is:

after

Question 12

Complete

Mark 0.00 out of 1.00

Which multiple access techniques is used by IEEE 802.11 standards for wireless LANs?

- a. CSMA/CD
- b. ALOHA
- c. CSMA/CA
- d. CSMA

The correct answer is:

CSMA/CA

Question **13**

Complete

Mark 1.00 out of 1.00

In slotted ALOHA, the vulnerable time is _____ the frame transmission time.

- a. half of a frame transmission time
- b. twice of a frame transmission time
- c. None of these
- d. same as the a frame transmission time

The correct answer is:

same as the a frame transmission time

Question **14**

Complete

Mark 1.00 out of 1.00

What are not the responsibilities of the Data link Layer?

- a. Framing
- b. Error detection
- c. MAC addressing
- d. IP addressing

The correct answer is:

IP addressing

Question 15

Complete

Mark 0.00 out of 1.00

The technique of temporarily delaying acknowledgements so that they can be hooked onto the next outgoing data frame is called

- a. Cyclic redundancy check
- b. Piggybacking
- c. Parity check
- d. None of these

The correct answer is:

Piggybacking

Question 16

Complete

Mark 1.00 out of 1.00

To avoid collisions on wireless networks, _____ was invented.

- a. CSMA/CD
- b. CSMA/CA
- c. Ethernet
- d. None of these

The correct answer is:

CSMA/CA

Question 17

Complete

Mark 0.00 out of 1.00

Which of the following protocols is the bit-oriented protocol?

- a. SSL
- b. All of these
- c. HDLC
- d. HTTP

The correct answer is:

HDLC

Question 18

Complete

Mark 1.00 out of 1.00

Transmission data rate is decided by _____.

- a. network layer
- b. transport layer
- c. physical layer
- d. data link layer

The correct answer is:

physical layer

Question 19

Complete

Mark 0.00 out of 2.00

The sender employs the "Go Back 10 ARQ" scheme. A 50 Kbps link has a propagation speed of 2×10^8 m/s. The transmitter and receiver is at 2000 km distance from each other. Each frame is 100 bytes long, assuming no transmission delay what will be the minimum round trip time delay for transmission of 1 million bits?

- a. 10 ms
- b. 50 ms
- c. 20 ms
- d. None of these

The correct answer is:

20 ms

Question 20

Complete

Mark 1.00 out of 1.00

In Carrier Sense Multiple Access which node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.

- a. Non-persistent
- b. O-persistent
- c. P-persistent
- d. 1-persistent

The correct answer is:

Non-persistent

Question 21

Complete

Mark 0.00 out of 1.00

The functions of _____ layer in the OSI model are handled by the transport layer itself in TCP/IP.

- a. presentation and session
- b. transport layer and session
- c. network layer and presentation
- d. application layer and session

The correct answer is:

presentation and session

Question 22

Complete

Mark 0.00 out of 1.00

The length of theof a specific packet will depend on the number of earlier-arriving packets that are queued and waiting for transmission onto the link.

- a. Queuing delay
- b. None of these
- c. Transmission delay
- d. Propagation delay

The correct answer is:

Queuing delay

Question 23

Complete

Mark 1.00 out of 1.00

The time required to examine the packet's header and determine where to direct the packet is part of _____

- a. Queuing delay
- b. Processing delay
- c. Propagation delay
- d. Transmission delay

The correct answer is:

Processing delay

Question 24

Complete

Mark 0.00 out of 1.00

Which of the following statement is correct for Slotted Aloha

- a. require global time synchronization
- b. divide time into discrete time intervals and also requires global time synchronization
- c. None of these
- d. divide time into discrete time intervals

The correct answer is:

divide time into discrete time intervals and also requires global time synchronization

Question 25

Complete

Mark 1.00 out of 1.00

Which of the following statement is incorrect, if the transmission bandwidth of a shared broadcast media of 50 Mbps is shared by 500 users then,

- a. Using CDMA scheme, each of the users have an access to 100 Kbps of bandwidth
- b. Using FDMA scheme, each of the users have an access to 100 Kbps of bandwidth
- c. Using CDMA scheme, each of the users have an access to 50 Mbps of bandwidth
- d. Using TDMA scheme, each of the users have an access to 100 Kbps of bandwidth

The correct answer is:

Using CDMA scheme, each of the users have an access to 100 Kbps of bandwidth

Question 26

Complete

Mark 0.00 out of 1.00

The _____ layer links network/user support layers by segmenting and rearranging the data.

- a. Network Layer
- b. Application Layer
- c. Session Layer
- d. Transport Layer

The correct answer is:

Transport Layer

Question 27

Complete

Mark 1.00 out of 1.00

A three-layer switch can be called as.....

a. Bridge

b. None of these

c. Repeater

d. Router

The correct answer is:

Router

Question 28

Complete

Mark 0.00 out of 1.00

Which of the following statements is not applicable for cable internet access?

a. It includes Hybrid Fiber Co-axials

b. It is a shared broadcast medium

c. Cable modem connects home PC to Ethernet port

d. Analog signal is converted to digital signal in DSLAM

The correct answer is:

Analog signal is converted to digital signal in DSLAM

Question **29**

Complete

Mark 1.00 out of 1.00

What is the role of logical link control sublayer in layer 2?

- a. Connection Establishment
- b. Sequencing
- c. Error detection
- d. Acknowledgment

The correct answer is:

Error detection

Question **30**

Complete

Mark 0.00 out of 1.00

What is the primary purpose of a virtual local area networks?

- a. Demonstrating the proper layout for network
- b. Simulating a network
- c. Segmenting a network inside a switch or device
- d. To create a virtual private network

The correct answer is:

Segmenting a network inside a switch or device

Question **31**

Complete

Mark 1.00 out of 1.00

In _____, each station is forced to send only at the beginning of the time slot.

- a. Slotted Aloha
- b. CSMA/CA
- c. CSMA/CD
- d. Pure Aloha

The correct answer is:

Slotted Aloha

Question **32**

Complete

Mark 1.00 out of 1.00

In reference to OSI model, TCP/IP model does not have _____

- a. application layer
- b. transport layer
- c. session layer
- d. network layer

The correct answer is:

session layer

Question **33**

Complete

Mark 1.00 out of 1.00

What are not the responsibilities of the Network Layer?

- a. Path determination
- b. Framing
- c. IP addressing
- d. Routing

The correct answer is:

Framing

Question **34**

Complete

Mark 0.00 out of 1.00

Which is true for Circuit Switching?

- a. The bandwidth used is not fixed.
- b. The bandwidth used is not fixed.
- c. All true
- d. The bandwidth used is not fixed.

The correct answer is:

The bandwidth used is not fixed.

Question **35**

Complete

Mark 1.00 out of 1.00

What is the total vulnerable time value of pure Aloha?

- a. T_{fr}
- b. None of these
- c. $\frac{1}{2} T_{fr}$
- d. $2 \times T_{fr}$

The correct answer is:

$2 \times T_{fr}$

[◀ Announcements](#)

Jump to...