3/07/2024 Wednesday

COMPUTER NETWORKING

– Dr. B. Rambabu Sir

TEXT BOOK : Andrew S Tanenbaum Computer Network

* Introduction:

- Many processors are interconnected on motherboard, but, it cannot be called as a network (or computer network) because they share a "master/slave" relationship, i.e, one processor or OS manages all other processors.
- A computer network is a collection of independent systems or processors or computers which are interconnected to each other through request-based relation.

Tightly-coupled architecture ⇒ all processors are connected on motherboard (Computer)

Eg: Mobile phone, IT architecture

Loosely-coupled architecture ⇒ all processors are loosely connected, i.e, located at different places.

CO → Single-processor Architecture

Multi-processor architecture ← tightly-coupled architecture
loosely-coupled architecture

In 4G, VOLTE → voice over LTE
↓ ↳ Long-Term Evaluation
Voice modulation and demodulation
Advantage – voice clear

4G ⇒ 6-8 MB/s
5G ⇒ 30-40 MB/s
} speed

Protocol Stack ⇒ software

3G → Web browsing (no video calls because 3G speed doesn't support it)
4G → video calls
5G → VR & AR

3G to 5G ⇒ speed & quality improved

Wi-Fi software ⇒ wireless Lan software → to check whether our phone can be connected to wi-fi or not
Bands ⇒ to see whether our phone is 3G or 4G or 5G
check bands

04/07/2024 Thursday

ISP → Internet Service Provider
SLA → Service Level Agreement

- SLA is called as FUP (Fair-Usage Plan).

In 4G, 2GB per day with 6-8 MB/s speed.
2GB per day unlimited means, after 2GB limit is completed, we get internet but at default 512 KB/s speed.

- Ethernet port in laptop is called as wired LAN (Ethernet software)
- The connector used in Ethernet port is called RJ22. (USB also)
- Ethernet is called wired LAN software.

Wi-Fi → wireless Fidelity
Wi-Fi ⇒ IEEE802.11 (wireless LAN software)

Ethernet software ⇒ IEEE802.3 (wired LAN software)

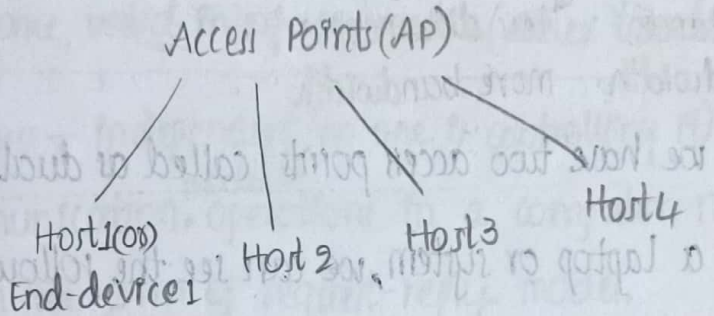
Fibers → Fiber box → Fiber & Ethernet port → Wi-Fi Router → will assign an IP address

- Mobile phones have '2' types of Networking softwares:

(i) Wi-LAN (or) Wi-Fi → connects to wi-fi (wireless) router

(ii) Bluetooth ⇒ IEEE802.15 → connects to other wireless devices like speakers, etc.

- In a centralised system, we have centralised system/device called as AP (Access Point) and hosts/end-devices.



SSID ⇒ Access Point Name

In centralised system, to connect we need authorisation or authentication, for that we need SSID and password and then IP address is obtained.
↳ will be discussed more in 3rd unit (router).

Mac Address — 48 bits — 6 × 8 ↳ 2 digit – 8 bits

IP Address — 32 bits (255.255.255.255)

In Mobile network settings, we have '2' types of settings, one is to connect automatically (It uses DHCP)

DHCP – Dynamic Host Configuration Protocol

⇓

If password is given, automatically we can obtain IP Address.

If DHCP is disabled, then IP address cannot be obtained automatically.

Gateway → Giving an IP address to our router and sharing it with family members

wireless Intercom ⇒ phone connected to router, router connected to laptop, we can directly access harddisk of laptop from phone instead of connecting to it. Because router's work is only to route data b/w devices.

- Fiber optic
- Coaxial cable
- twisted-pair wires

} All these transmission media have different characteristics

- Near Field communication ⇒ Alternative for IR
- Wi-Fi Router ⇒ 2.4 - 5 GHz

2.4 → more distance, less bandwidth
5 → less distance, more bandwidth

For Jio fibernet we have two access points called as dual bands.

- While purchasing a laptop or system, we can see the following:
  (i) System configuration (RAM)
  (ii) GPU or multimedia card (for Graphics)
  (iii) Processor (multi-processor architecture or not)
  (iv) Storage (SSD or Harddisk)
  (v) Wi-fi enabled or not
- End-point is the process running in our system. End-point need not be a system.
- Reliable - no data loss

UNIT-1. INTRODUCTION

* Uses of Computer Networks: (Short Answer Only)

* Computer Networks (definition):

Interconnected autonomous computers is called computer network.

Two computers are interconnected to exchange the information/data through some valid interface/media (either wired or wireless).

- Autonomous – independent (no one is controlling it)
- The communication model or operations in a computer networking are always in the form of request-reply model.
- No master-slave relation in a computer network.

  ⇓

  Eg: In multi-processor architecture or system, all processors are connected on a single motherboard but they are controlled by a single-unit called as control unit.

Eg of Computer network: Internet, Intranet, Ethernet, Lo-Lan (copper Lan - Lor-fi)

30/07/2024 Wednesday

* Uses of Computer Networks:

Traditional uses at Companies and for individuals are (and then move to recent development regarding mobile users and home networking):

(i) Business applications:

- ~~(i)~~ resource sharing
  - → resource an be a software or hardware.
  - → using CN, we can provide resource availability to users though resource is located somewhere (remote).
- (ii) sharing information

The systems/computers may be in single building/scattered across vast area.

- Client-server model:

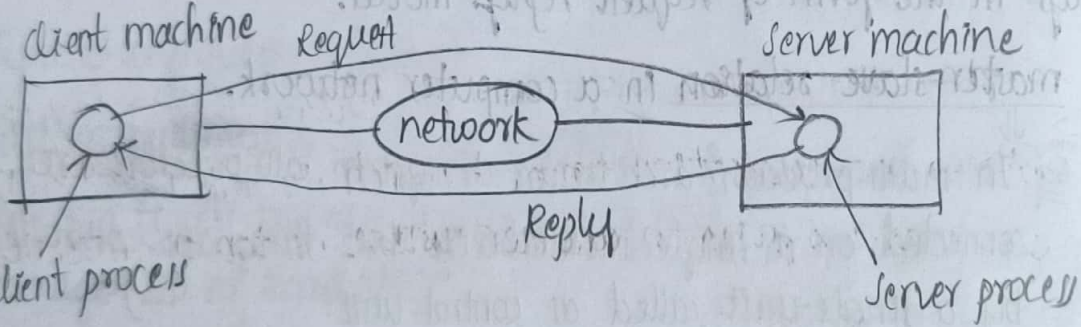
→ Server is a system to provide information ~~to a cli~~ upon request from a client.

→ Client is a system/machine which sends request to server.

Web2.0 ⇒ fb like client-server model

centralised → backend - server
→ frontend - client

Web 3.0 architecture ⇒ distributed approach
(no centralised architecture)



~~for~~ Two processes ⇒ client process, server process
Two messages ⇒ Request message, Reply message

- Communication medium:

→ It can be e-mail, instant messaging, chat

- Collaborative work:

→ working together sitting at different locations

- Videoconferencing & audio-conferencing:

→ shared virtual blackboard

- E-commerce:

→ doing buiness electronically with other companies, suppliers and customers.

→ doing buines with consumer over internet.

(II) Home applications:

Popular use of the network internet for home users are:

- Access to remote information → surfing WWW
- Person-to-person communication
- Interactive entertainment
- Electronic commerce

Internet → eg of computer network which provides communication interface/service.

World wide web (WWW) → software or application built using CN or internet

url → the system with that IP address at that location

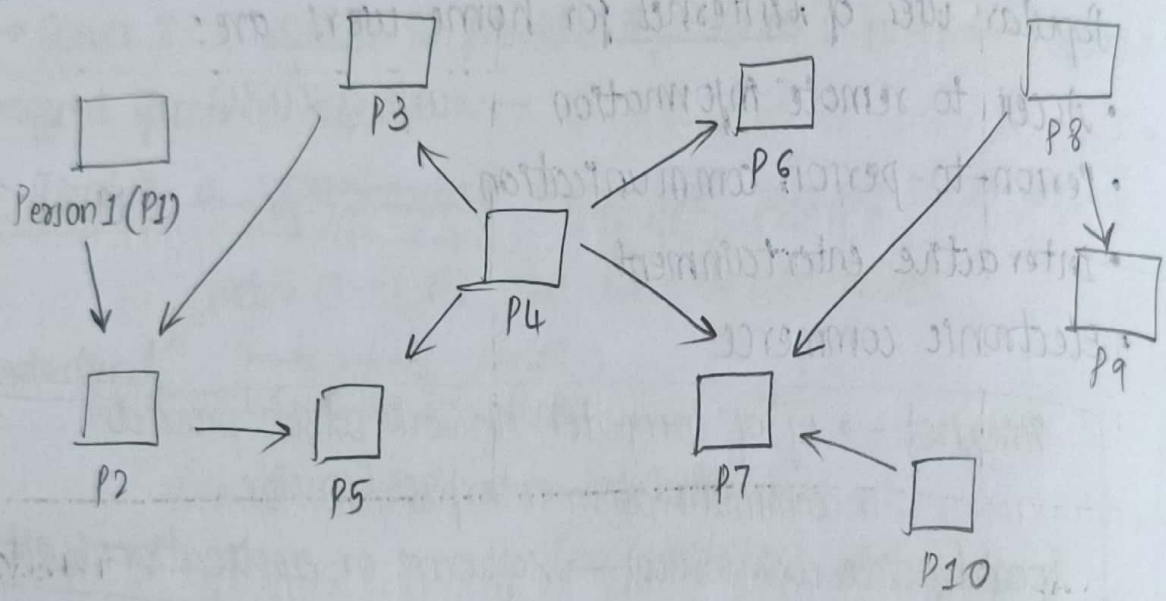
http → communication protocol which transfers info from one system to another system on top of internet.
↓
HypeText Transfer Protocol

DApps → apps developed on top of Distributed systems

Web Apps → apps developed on top of internet

- access to remote information ⇒ surfing WWW
  - → online-digital library
  - → cooking, art, etc. videos
- person-to-person communication → E-mail
  - → instant messaging
  - → chat room
  - → worldwide newsgroups
  - → peer-to-peer communication
  - → ~~client-server model~~

Peer-to-peer communication/network/systems:



Peer-to-peer ⇒ peer-level entities (same-level entity)
↓
same functionality

The next generation of the peer-to-peer systems eliminates the central database by having each user maintain his own database locally.

Use-cases of Internet → telephone calls, video, phone, Internet radio, telelearning

- Interactive entertainment → video on demand (Netflix)
  → audio on demand (Spotify)
  → movie streaming
  → online quiz
  → multi-person real-time simulation games

- Electronic commerce/E-commerce → financial institutions
  → online auctions

Some forms of e-commerce

-

~~Tag~~ Some forms of E-commerce:

Tag	Full Name	Example
B2C	Business-to-Consumer	Ordering books online
B2B	Business-to-Business	Car manufacturer ordering tires from supplier
G2C	Government-to-Consumer	Government distributing tax forms electronically
C2C	Consumer-to-Consumer	Auctioning secondhand products online
P2P	Peer-to-peer	File sharing

11/07/2024 Thursday

(ii) Mobile Users:

- Mobile computers:

  Eg: Laptop, PDA

- Wireless networks:

- ~~Re~~Portable office
  - work from home

- Wireless networks are also important to the military.

TB (Fig-1.5)

(iii) Social Issues:

- Networking has introduced new social, ethical and political problems.

* Network hardware:

- Technical issues involved in network design.
- Two dimensions:
  (i) Transmission technology
  (ii) scale (size)

} Network hardware is broadly discussed in two dimensions

2 Marks Ques.

• There are two types of transmission technology:

(i) Broadcast links } Short Answer Ques's
(ii) Point-to-point links }

~~• Broadcast networks ..... ; it is just ignored.~~

* Broadcast links:

Broadcast → announcements

→ Broadcast networks have ~~ram~~ a single communication channel, that is shared by all the machines on the network.

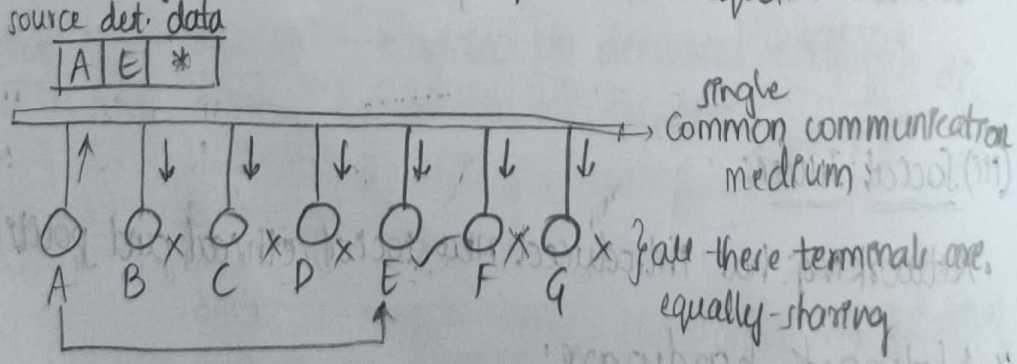
→ short messages, called packets in certain contexts, sent by any machine are received by all others.

→ An address field within the packet specifies the intended recipient.

→ Upon receiving a packet, the machine checks the address field.

→ If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored.

equal sharing → no priorities, everyone are equal.



NOTE: Also called as multi-point communication (because communication medium has multiple points connecting to terminals).

Communication operations are of three types:

(i) Broadcast communication → message/packet reaching all terminals
(ii) Multicast communication → message/packet reaching subset of terminal
(iii) Unicast communication → message/packet reaching only one terminal

- When you are sending to all, we use special destination address (like all 1's).
- When you want to send messages to a group of people, we use group address (denoted by 'R') as destination address.
→ We use group management software on top of CN to manage these groups and group addresses and group activities.
- When you want to send messages to a single person (or terminal), we use destination terminal's address.

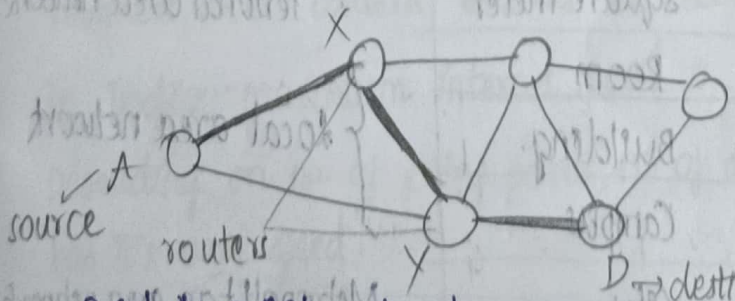
* When multiple users/terminals try to send data (or signals) at the same type then collision of data (or signals) occurs.

collision → overlapping of data
⇓
It leads to data loss

- Link is shared in Broadcasting links.
- Link is dedicated/exclusive b/w two terminals in point-to-point links

MAC → Medium Access Control
↳ Communication media
↓
It is used for two-way communication to avoid collision

- Point-to-point links/networks/transmission technology:



Intermediate terminals are called as routers or switches because they transmit data to the destination on behalf of source

→ Point-to-point networks consist of many connections b/co individual pairs of machines.

→ To go from the source to the destination, a packet visit one or more intermediate machines.

→ Multiple routes, different lengths. So, finding good one is important.

→ smaller, geographically localized networks tend to use broadcasting, larger networks use point-to-point.

→ one-sender and one-receiver — ~~Un~~ called as unicasting.

→ Collision occurs in broadcasting links but no collisions in point-to-point links. But multiple routes in point-to-point, so finding optimal route is quite challenging.

→ Based on destination address, we can also have broadcast, multicast and unicast in point-to-point links.

***
* Classifying networks based on scale:

Long Ans Ques
*****

IMP
IOM

scale → size

- personal area networks
- meant for one person
- a computer with its mouse, keyboard,

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10000 km	Planet	The internet

12/07/2024 Friday

ISP → Internet Service Provider

They manage the internet

Local ISP ⇒ they manage internet within that locality, i.e, they manage local networks

↑

Regional ISP ⇒ they manage group of local networks, i.e, networks of various towns

↑

National ISP ⇒ Eg: BSNL, Jio, Airtel

They manage national-wide or country-wide networks

↑

World-wide networks ⇒ Interconnection of national ISP's.

Every entry is monitored by Government of India (Telecommunication department of India).

Tik-tok is banned — How? ⇒ We have gateways/entry points to get data from various national ISP's, at that gateway firewall is inserted and content is filtered. In this way Govt. of India, monitors what content should we recere.

India has '4' entry points ← Chennai, Mumbai

In India, maximum internet speed is 10MB/s.

Depending on no. of entry points, no. of connections, every country has it's own speed.

submarinecable.com

---

(1) Personal area network (PA):

→ Deals with collection of personal badges - personal computers like a keyboard, mouse, etc. to computer.

→ Covers area of 1 sq.m and they are seperated with a distance of 1m.

(1) Local area network:

→ They are called LAN's.

→ They are privately owned network.

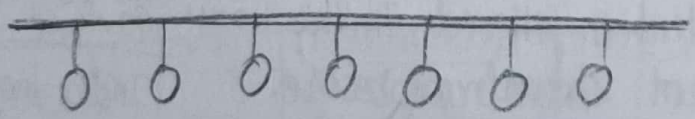
→ They are established within a room, building or campus.

→ They are seperated by 10m to few km (1 km).

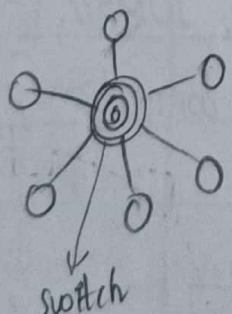
→ These personal LAN's are used to connect ~~to~~ personal computers, to workstations and company offices, to share resources and ~~information~~ exchange the information.

Every network has three characteristics to differentiate or distinguish from others:

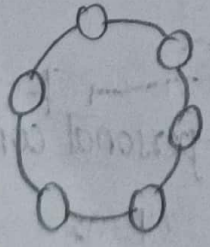
- their size ⇒ no. of systems on a geographical area
- their transmission technology < broadcasting links — LAN's are this type
  point-to-point links
- their topology ⇒ where the systems are connected
  ↓
  The physical arrangement of systems and their connections.



⇒ Bus topology



⇒ Star topology
(20-30 systems)



⇒ We use this when we have less no. of systems (10 systems)

LAN: → size

→ size - 100 systems

→ broadcasting links → transmission technology

→ Bus topology → topology

WAN (wide-area network):

→ size (spans over lakhs of km)

→ point-to-point links

→ ~~netw~~ Graph topology

CAN → Control Area Network

Eg: Kia Cars, automobiles

→ less than 1 meter

Geo Fencing → using this app, we can control upto how much dist. our engine can be turned on., we can avoid thefts. within our mentioned location only we can run our car

Monday

15/07/2024

→ LAN's are restricted in size, i.e, the worst-case transmission time is bounded and also known in advance.

→ LAN simplifies network management.

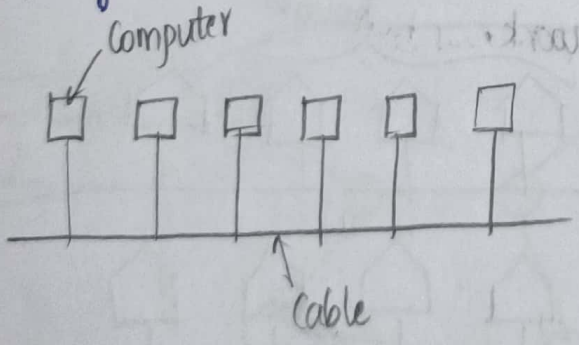
→ LAN speed ranges from 10 Mbps to 100 Mbps and have low delay (microseconds or nanoseconds).

→ Newer LAN's operate at up to 10 Gbps.

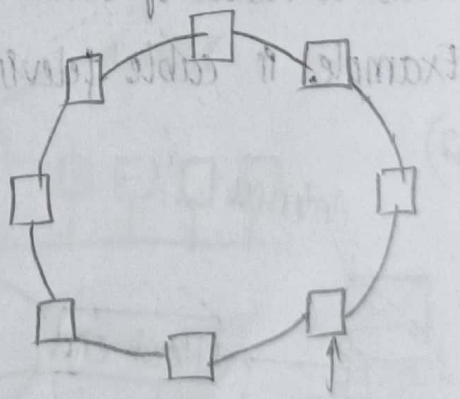
→ The topologies feasible or possible for broadcast LAN's are:

(i) Bus

(ii) Ring



(a) Bus



(b) Ring

• In a bus, at any instant almost one machine is master and allowed to transmit. Other machines refrain from sending. Arbitration mechanism is needed to resolve conflicts when two or more machines want to transmit simultaneously. Arbitration mechanism may be centralized or distributed.

• Eg: IEEE802.3, called Ethernet, is a bus-based broadcast network with decentralized control usually operating at 10Mbps to 10Gbps. Ethernet can transmit whenever

(Pg-21)

• A second type of broadcast system is the ring.

• Eg: IEEE802.5 (the IBM token ring), is a ring-based LAN operating at 4-16 Mbps. FDDI is another example of a ring network.

• Broadcast networks can be further divided into static and dynamic, depending on how the channel is allocated.

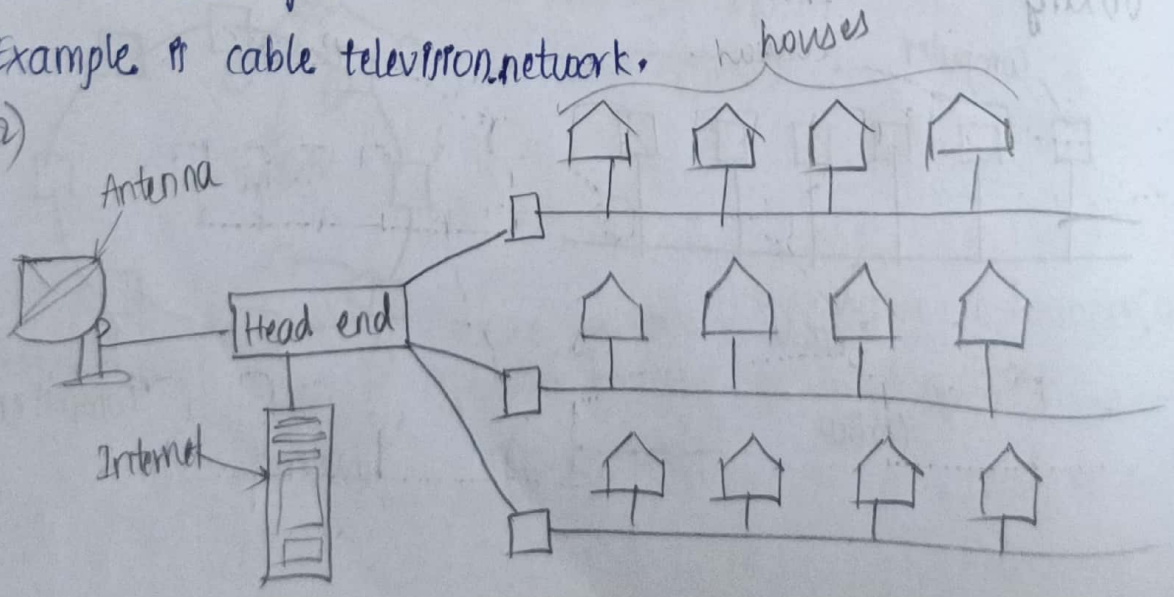
(iii) Metropolitan Area Networks (MAN):

→ It covers the city.

→ Covers a radius of 30km.

→ Example is cable television network.

(Pg-22)



• high-speed wireless internet access recalled as another MAN, IEEE 802.16.

IEEE 802.11 ⇒ Wi-Fi (extended upto few meters)

IEEE 802.15 ⇒ Bluetooth

Wi-Max ⇒ IEEE 802.16 ⇒ wireless broadband connection extended upto few km.

city-level wireless network

(iv) Wide Area Networks (WAN):

→ WAN spans a large geographical area, often a country or continent.

→ Country-level network.

→ It has two types of systems:

(i) Host (end-user systems) (Eg: Mobile phones)

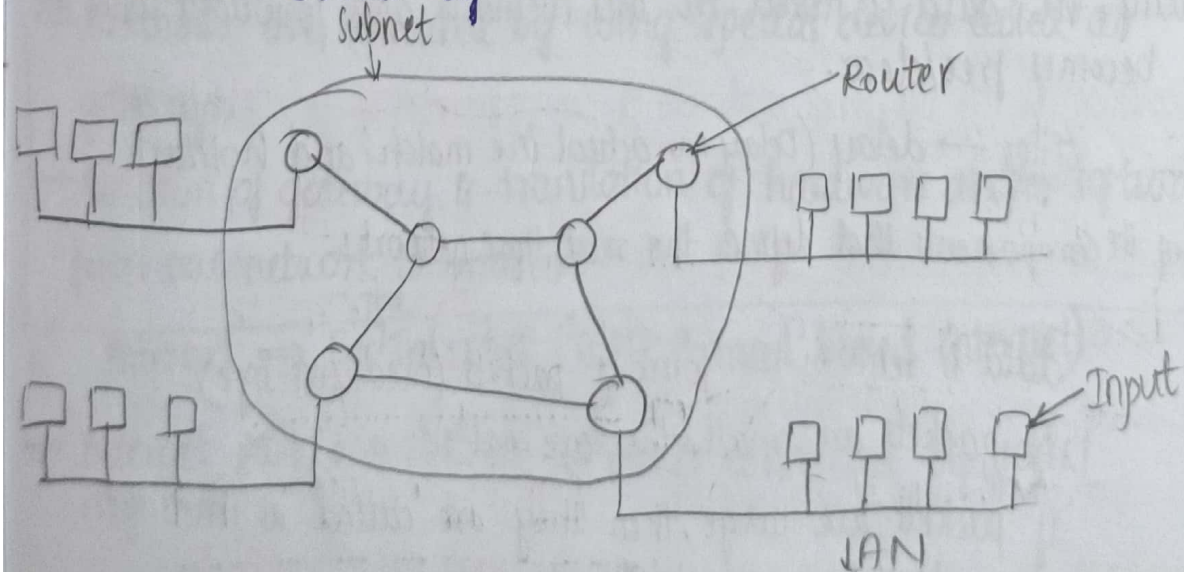
(ii) subnetwork (Eg: Airtel Operator)

↳ part of network that carries information from one system to another.

→ WAN contains collection of machines intended for running user (i.e, application) programs, called as hosts.

→ Hosts are connected by a communication subnet.

→ Hosts are owned by customers.



→ Subnet consists of two different components:

(i) transmission lines → wired or wireless

(ii) switching networks / routers / switches / intermediate terminals

Transmission line — moves bits b/w machines

— copper wire, optical fiber or even radio links

Switching elements — specialized computers that connect three or more transmission lines

— when data arrives in incoming line, the switching element chooses outgoing line to forward data.

→ In fig., each host is frequently connected to a LAN on which a router is present. In some cases host can be directly connected to router.

Fig-1-10 (a) TB

• WAN's uses store-and-forward technology.

Network queues ⇒ Network memory

↓

Every system or router has their extra storage. If the line/link is busy, the data is stored in this memory and forwaded when the line becomes free/clear.

Jitter → delay (Delay in actual line match and holstar).

↓

One of the components that define the real-time networks

data is sent in the form of packets (medium-size)

If packets are small, they are called as 'cells'

If packets are large, then they are called as messages.

Message → set/collection of packets

↳ set/collection of cells

18/07/2024 Thursday

Principle of Packet-switched WANN's:

packet → group of bits with proper header

- acts the message into packets, each one bearing its number in sequence.
- injected into the network
- transported individually
- reassembled into the original message

→ Every packet need to numbered (sequence-numbered) (a unique identifier number to that packet.)

→ there is ordering of packets if the packets follow multiple paths.

* Wireless Networks:

Wireless networks can be divided into three main categories:

- System interconnection (wireless PAN's - wireless mouse, keyboard, etc.)
- Wireless LAN's (Wi-Fi) (IEEE802.11) (One access point - all devices connected to it)
- Wireless WAN's (Wi-MAX) (IEEE802.16)

(v) (vi) ~~(vi)~~ Inter Networks:

→ Internet is called as interconnected collection of networks. (interconnected collection of systems)

→ Networks (different) are connected by using special devices called as gateways.

→ Function of gateway is translation of hardware and/or software from one network to another.

Internet ⇒ Eg: The Internet (TCPIP Protocol based Internet)

→ Internet ~~⇒~~ is a collection of LAN's connected by WAN.

* Network Software:

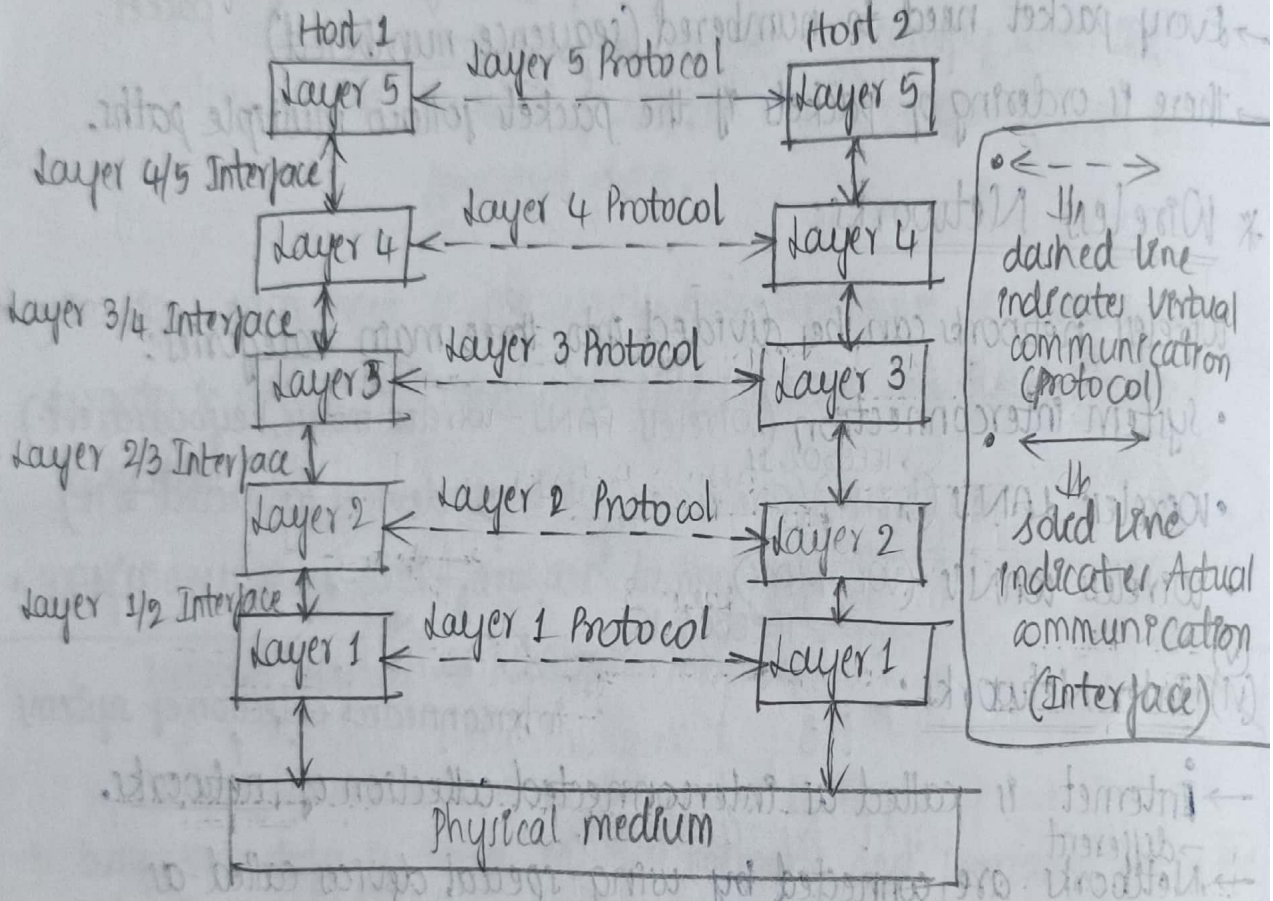
* Protocol Hierarchies:

1M Ques — like grammar

→ Protocol is a set of rules agreed by two communication parties on how to communicate.

→ Layer: It is a module in a software project

Layered Architecture: Headless — 1M Ques



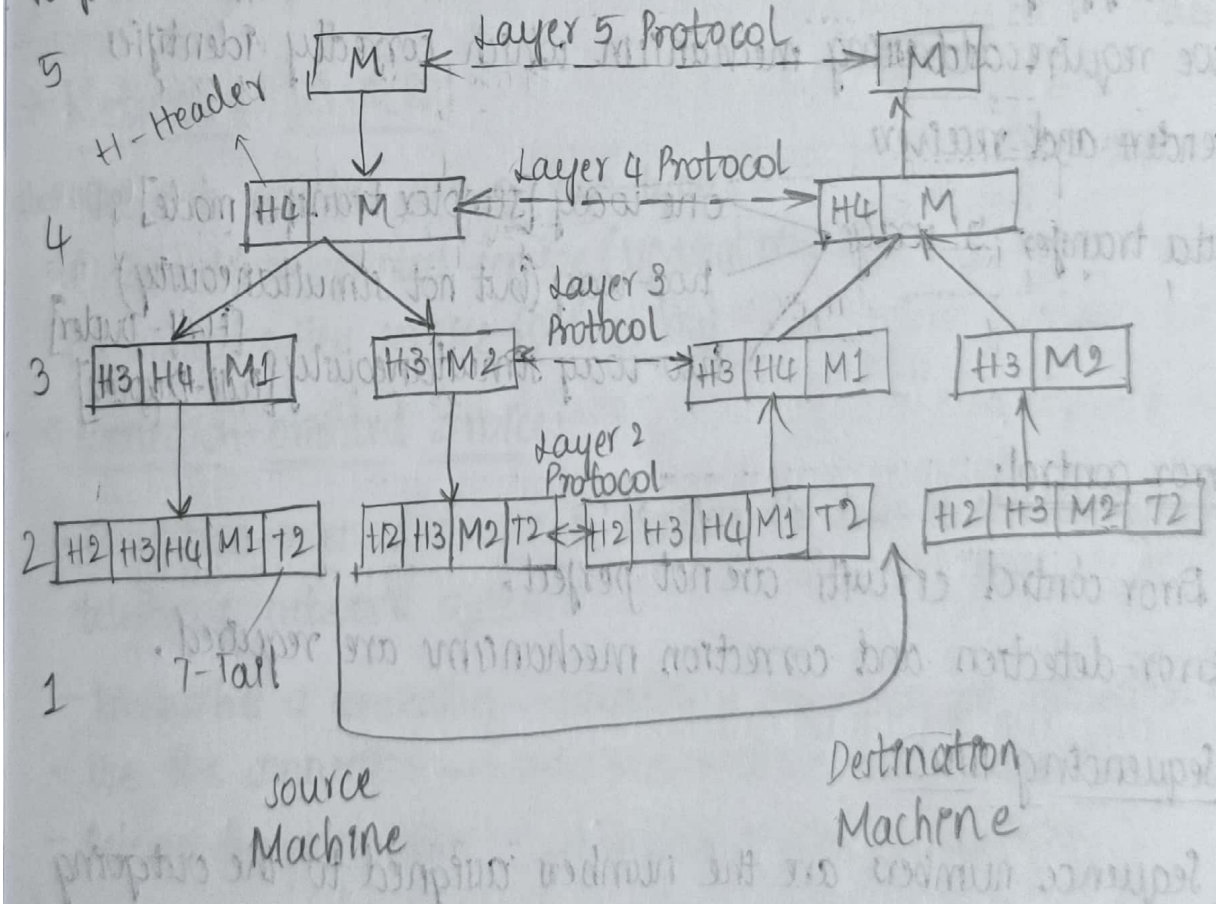
- A collection of layers and their corresponding protocols is called network architecture.
- ~~Network architecture~~ — It is also called protocol stack or network protocol stack. (list of protocols used by a certain system)
- Protocols are applied on entities of different machines which are at same level. (peer-level entities — peer-to-peer communication)
- Interface is the communication interface or set of rules

which enables communication b/w adjacent layers or entities of same machine.

- Virtual communication b/w peer-entities is by protocol.
- Actual communication b/w adjacent layers is by interface.
- Protocol information is exchanged with the help of a header.
- Each layer has a specific name, specific functionality.
- Each layer offers the services to the upper layer, but, it uses the services of the lower layer.

Data exchange in layered architecture:

PI (Protocol Information) → set of rules applied on incoming data



MTU → maximum Transmission Unit / Maximum Processing Unit

'M' → H4 M

↳ H4 contains PI

22/07/2024 Monday

* Design issues for the layers in a network: IM Ques

To develop/design a layer or network, we need:

(i) Users or computers

(ii) Connections among them

(iii) unique addres to each layer

(iv) Error detection and correction
(Due to fault in transmission links data may get deleted or added, etc.)

(v) Decision making software inorder to route data to correct destination.

(i) Addressing issue:

- Identifying senders and receivers
- We require addressing mechanism which correctly identifies senders and receivers

Data transfer 3 ways:
- one-way [simplex transfer mode] Eg: FM Radio
- two-way (but not simultaneously) [Half-Duplex]
- two-way simultaneously [Full-Duplex]

(ii) Error control:

- Error control circuits are not perfect.
- Error-detection and correction mechanisms are required.

(iii) Sequencing issues:

- Sequence numbers are the numbers assigned to the outgoing data units (packet numbers).
- They help in ordering of messages.

(iv) Flow control issue:

- Flow control ~~dealing~~ deals with controlling speeds at different terminals.

(v) Maximum transmission unit:

- Maximum transmission unit deals with the segmentation and reassembling of messages.

(vi) ~~Separate conne~~

- Multiplexing deals with n-inputs going to one output.
- Demultiplexing deals with dividing one ~~output~~ input into n-outputs.

(vii) Multiple paths exist b/w source and destination. So, an optimizing mechanism is required to choose best path.

23/07/2024 Tuesday

* Network services:

Network services are of two types:

(i) Connection-oriented service (virtual circuit)

(ii) Connectionless service (Datagram)

* Connection-oriented service:

- Connection-oriented service is similar to ~~tele~~ a service offered by telephone network system.

- Establishes a connection → Establish a connection (or) connection setup
- Uses ~~the~~ connection → Data transmission using connection
- Releases the connection → Connection release or terminate.

→ No master/slave relation, it is always autonomous (request-based relation).

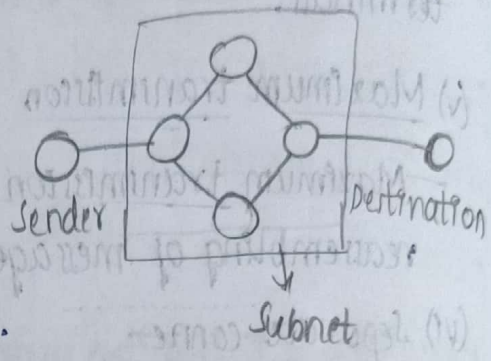
→ Connection is just like a tube, sender pushes objects (bits) in at one end, receiver takes them out at the other end. The order is

preserved, bits arrive in the order.

- Connection setup
- communication establish

Quality of service → Expectation

→ When a connection is established, the sender, receiver and subnet conduct a negotiation about the parameters to be used, such a maximum message size, quality of service required and other issues.



* Connectionless service:

- Connectionless service is a service offered by a postal system.
- Each message carries the full destination address, and each one is routed through the system independent of all the others.

→ Every ~~path~~ packet need not follow same path, every packet is sent through different route independently. (Independent routing)

- Two messages - same destination, first one sent can be delayed, the second one may arrive first.

→ In connectionless, every packet contains full destination address and every packet is routed independent.

→ There are multiple paths are used for a given pair of source and destination.

→ Packets may be out of order.

* Each service either connection oriented or connectionless can be characterized by a quality of service.

- reliable services — never loose data.
- Reliable service - receiver acknowledges the message.
- Quality of service is offered by acknowledgement (feedback) service.

• If there is an Acknowledgement from destination to the source, then we call it as reliable service.

• If there is no acknowledgement, then we call it as unreliable service.

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitalized voice
Connectionless	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

client-server → mostly they are reliable

Fig: Six different type of service (Pg-33)

24/07/2024 Wednesday

TCP → Reliable byte stream Protocol

Transfer Control Protocol

Telegram (phone) ⇒ voice-based service

Datagram ⇒ communication network

Telegram ⇒ passing information (like FAX)

• Datagram means a connectionless service network.

• When we have acknowledgement, it means we have reliability, i.e, no data is lost.

• Reliable services are slow.

• Real-time applications, multi-media (mostly) use unreliable connectionless services.

Internet is successful because of 2 protocols

(i) TCP (Transfer Control Protocol)
↳ useful for FTP (File Transfer Protocol also)

(ii) UDP (User Datagram Protocol)
↳ connectionless (speed)

1M Ques

* Service primitives: (Primitive operations for connection-oriented services)

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection.

Fig: 1-17. Five service primitives for implementing a simple connection-oriented service

Connection setup ⇒ comprises of LISTEN, CONNECT
Data transfer ⇒ comprises of RECEIVE, SEND
Termination ⇒ DISCONNECT

* Primitive operations for connectionless services are:
- SEND
- RECEIVE

★★★★★ (5 star Ques)

Communication Models:

- OSI Model
- TCP/I Model

} we get atleast one of these in mid

* OSI Reference Model:

★★★ 10M Ques

- OSI stands for "Open System Interconnection".

→ It is interconnection of open systems.

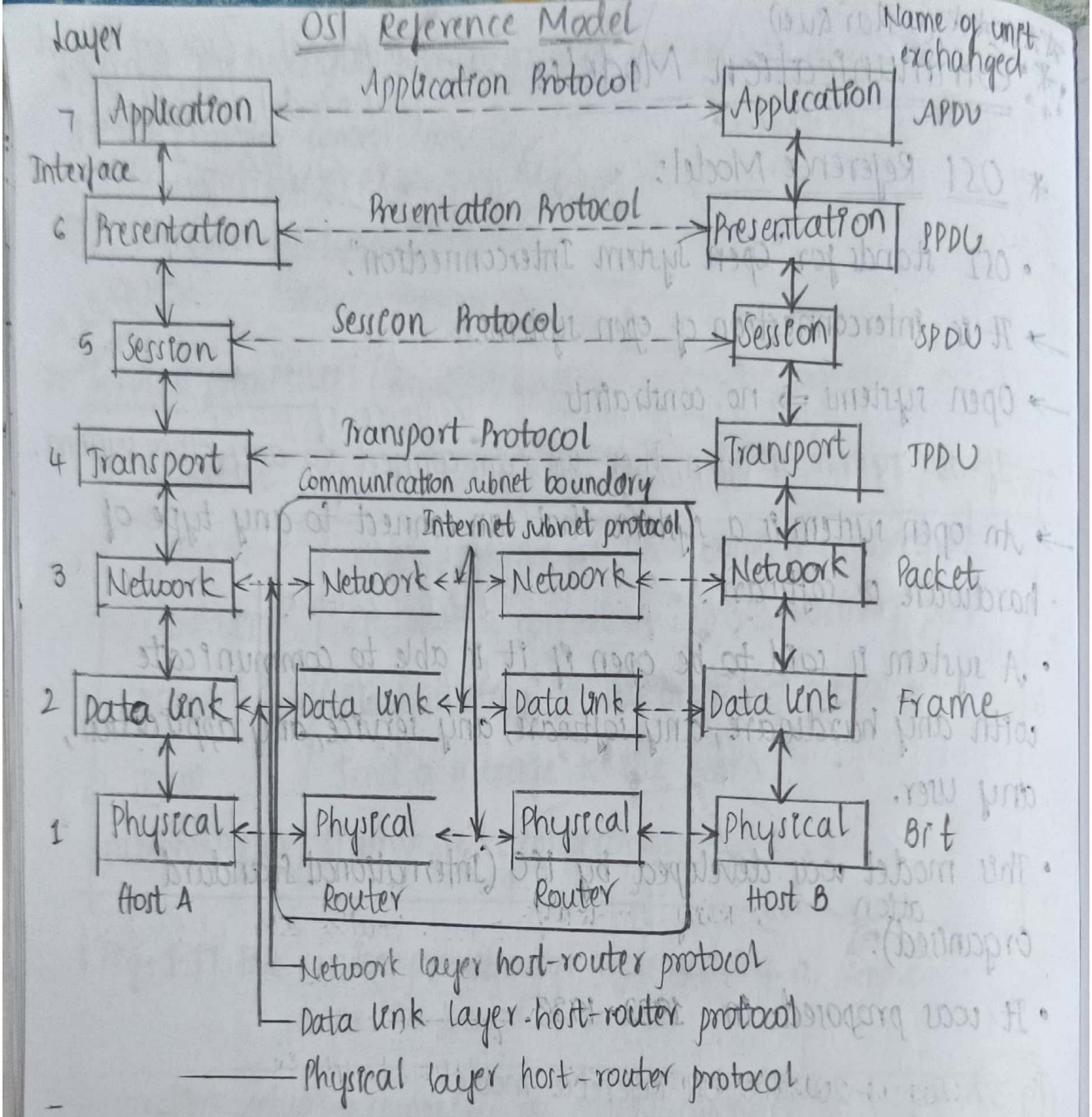
→ Open systems ⇒ no constraints

If our system is open, then we can connect to any other system.

→ An open system is a system that can connect to any type of hardware or software.

- A system is said to be open if it is able to communicate with any hardware, any software, any service, any application, any user.
- This model was developed by ISO (International Standard Organisation).
- It was proposed in 1983-1985.

Pg-37 Fig: 1-20. The OSI Reference model



- OSI model has '7' layers: (Bottom-up approach in freq)

(i) Physical layer
(ii) Data-link layer
(iii) Network layer
(iv) Transport layer
(v) Session layer
(vi) Presentation layer
(vii) Application layer

Organisational network → subnetwork
- → Transmission links
- → Intermediate terminals (routers)

25/07/2024 Thursday

(i) Physical layer:

→ It deals with transmission of raw bits over a communication medium.

→ The functions/functionality of physical layer:
- data encoding and decoding

→ Data encoding technique deals with how to represent a binary '1' or binary '0' in communication medium.

Eg: Giving +5V (volts) for '1' and −5V for '0'

→ • Physical layer deals with data transfer.
- one-way (simultaneous)
- two-way (not simultaneous)

→ • Physical layer deals with different connectors (design of)
- USB, RJ45, C-type, etc.

RJ45 Connector ⇒ Ethernet port

Ethernet wire has a limitation of 10 GBps.

USB → Universal Serial Bus

→ • Physical layer deals with different types of connectors, how many pins and significance of each pin (Data pin, Power pin, Control pin).

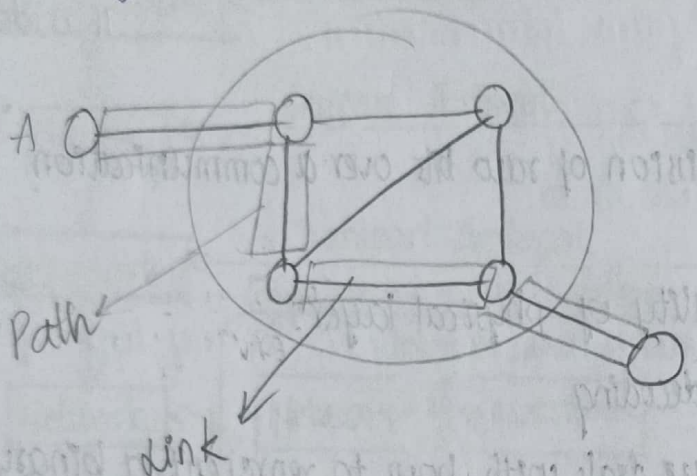
→ • Physical layer deals with mechanical, electrical, timing interface over a communication medium.

(ii) Data link layer:

→ Functionalities of data link layer:
- data (It is a data control layer) → data controlling b/w two adjacent terminals

• → Data link layer deals with controlling data over a link.

• → Link can be defined as the communication path or medium between two adjacent terminals.



The functionalities of data link layer:

• Error control:
  - deals with transmission errors
  - further it contains two different modules
    → Error detection algorithms (Eg: CRC algorithm) (Cyclic-Redundancy-Check code)
    → Error correction algorithms (Eg: Hamming code)

⇓

It can be a: self-healing solution → Error correction is done by destination itself
Feedback solution

⇓

Error correction is done by the feedback from destination to source

in the form of acknowledgement

⇓

'2' types

Positive ack. (data is received reliably)

Negative ack. (data is in corrupted format)

29/07/2024 Monday

→ If it is a positive acknowledgement, the source machine will continue with the next data unit transmission, otherwise (negative acknowledgement) source re-transmits the same data unit.

• Flow control:

→ Flow control deals with regulating the flow b/w diff. speed terminals.

SLA (Service Level Agreement) ⇒ Negotiation (eg: b/w customer and service provider)

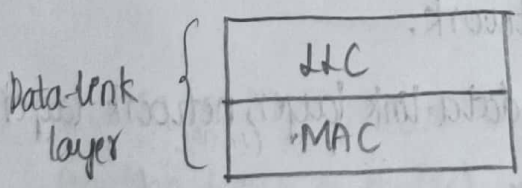
→ Flow control basically has '2' types of techniques:

- Parameter negotiation (SLA) (Negotiation on certain values like speed, etc.)
- Feedback negotiation (Stop & wait & continue algorithm)

• Access Control:

→ Data link layer is divided into two sub-layers:

- LLC (Logical Link Control)
- MAC (Medium Access Control / Multiple Access Control)



LLC deals with the transmission errors over WAN networks (point-to-point networks). It includes error control, flow control algorithms.

In a broadcast transmission technology networks, if two or more terminals or machines simultaneously access the common shared medium, then collision is occurred. Collision means overlapping of transmission/transmitted signals in a shared media. Collision is due to simultaneous access. So, we need a controlling mechanism.

to acces the shared media, that is called Medium Access Control (MAC) in data-link layer.

CSMA (Carrier Sense Multiple Access) Protocol

when many terminals transmit data, check whether channel is busy or free.

IEEE802.3 ⇒ Ethernet
IEEE802.4 ⇒ Token bus
IEEE802.5 ⇒ Token ring
IEEE802.11 ⇒ WAN
IEEE802.15 ⇒ Bluetooth
IEEE802.16 ⇒ Wi-Max

(iii) Network layer:

→ Network layer is the third layer.
→ Network layer belongs to the subnetwork.
→ The combination of physical layer, data-link layer, network layer are called subnetwork boundary layer.
→ A device which contains physical layer, data-link layer, network layer is called router or switch device.
→ Network layer is the core layer of the network architecture.

Functions or functionalities of network layer:

- Routing:

→ Routing means, it is a decision making software which decides what is the best output line for ~~the~~ a given incoming packet.

→ Routing is of two types:
- Dynamic routing
- Static routing

30/07/2024 Tuesday

→ Routing process contains two algorithms:
- Forwarding algorithm
- Routing algorithm

→ Forwarding algorithm - switching or forwarding the data or packet from one line to other line using routing table.

→ Routing algorithm - used to design the routing tables based on topology.

→ Routing algorithms are further devided into '2' types:
- Static routing algorithms - whatever may be the condition of the network you follow the same path (routing table is static)
- Dynamic routing algorithms - Based on the condition of the network, we choose the non-congested path (routing table is updated frequently/dynamically)

→ Static routing means the routing decisions are not changed (routing table is static).

→ Dynamic routing means the routing decisions are changed (routing table is updated dynamically/periodically based on the condition of the network).

more density area
• Congestion Control:

→ Congestion is defined as - if too many packets are present in the network, the performance of the network gradually decreases.

→ We require a congestion control to control the congestion. mechanism

• Internetworking:

→ It deals with interconnection / integration of existing networks.

→ The networks may differ in packet size, hardware, software, protocol, service or application.

→ Network layer is applicable to point-to-point or WAN networks.

→ Network layer offers the host-to-host delivery.

(IV) Transport Layer:

→ It is a layer that transports data packets from source to destination.

→ Transport layer deals with the transportation of data from one process in one system to another process in another system.

→ Transport layer - offers process to process delivery
Network layer - offers system to system delivery

→ Transport layer offers end-to-end communication.

→ Transport layer is user layer. (It is present in host in osi model fig)
⇓
Only user terminal contains this layer
whereas subnetworks or routers are present in

31/07/2024 Wednesday

→ Functionalities of transport layer are similar to the data-link layer
(I) (II)
(error control, flow control)

→ Data link layer generally works on a link whereas transport layer protocols are applied on a subnetwork.

(III) → Transport layer offers multiplexing and demultiplexing.

(IV) → Transport layer offers the data recovery.

(V) → Transport layer offers buffering (queue management).

→ Transport layer basically offers '2' types of services:
(i) Connection-oriented service
(ii) Connectionless service.

(v) Session Layer:

→ Session layer functionality is similar to transport but the transportation of data in the form of sessions.

→ Sessions over various services like dialog control (keeping track of whose turn is it to transmit), token management (preventing two parties from attempting the same critical operation at the same time), and synchronization (checkpointing long transmissions to allow them to continue from where they were after a crash).

→ Examples of session oriented
- Dialog control
- Token management
- Synchronization

→ In token management, if more than one machine want to transmit data, the system which has token can transmit data, and all other systems are in listening mode.

(vi) ~~The~~ Presentation layer:

→ Syntax and semantics of the information transmitted.
- Syntax → Patterns
- Semantics → Meaning of the patterns

→ Presentation layer deals with the syntax and semantics of data/information transmission.

Eg: ASCII (8-bit), UNICODE (16-bit), compression algorithms, encryption & decryption algorithms

(vii) Application layer:

→ Application layer deals with different types of user applications like HTTP (HyperText Transfer Protocol), World Wide Web (WWW), FTP (File Transfer Protocol), E-mail (Electronic mail), R-login (Remote login - TELNET is one R-login application).

☆☆☆☆☆

* TCP/IP Reference Model:

5 star Ques

TCP ⇒ Transmission Control Protocol

IP ⇒ Internet Protocol

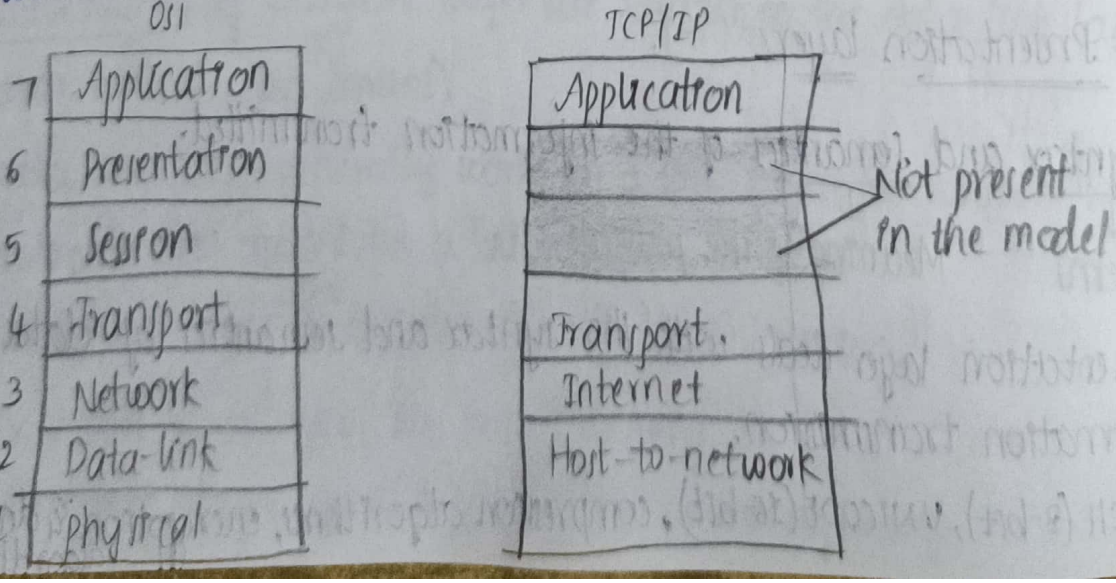
→ This model is also called Internet model.

→ The organisation is IETF (Internet Engineering Task Force) under IAB (Internet Architecture Board).

→ The primary goal of Internet model is how to connect the existing networks. That is called as Internetworking. (Integrate or Interconnect or)

→ ~~Internet based~~ a internet (collection of networks) based on OSI model is called as ARPANET (American Research Project Agency NET) which is owned by DOD (Department of Defense)

→ The OSI model failed when we tried to connect a wired network ~~is connected to~~ with wireless network like satellite



01/08/2024 Thursday

(I) Host-to-network layer:

→ It deals with physical and data-link layer of ~~netw~~ OSI model.

→ Host-to-network layer is the combination of physical and data link layer but ~~it doesn't describe about that layer.~~ this internet model doesn't

(II) Internet layer:

→ The network layer of OSI model is called internet layer as it deals with the internetworking.

Internet ⇒ interconnection of existing layers

→ Internet layer defines one official protocol called as IP protocol (Internet Protocol)

→ IP protocol is a connectionless and unreliable protocol.

→ TCP/IP networks are called datagram networks.

↓

It uses ~~follows~~ connectionless protocol

→ There are some other protocol:

- IP protocol
- ICMP (Internet Control Management Protocol)
  ↳ It offers services related to Internet management
- ARP (Address Resolution Protocol) } Address translation protocols.
- RARP (Reverse Address Resolution Protocol) }

→ In Internet layer, sender sends a message (PDU - Protocol Data Unit ~~called as~~ packet called as Datagram packet).

(III) Transport layer:

→ The functionality is similar to OSI model.

→ The functionalities are transport/networking services, error control, flow control, buffering, data recovery, multiplexing.

→ In Internet ~~layer~~ model, the transport layer follows defines various protocol.

- TCP (Tranfer Control Protocol):

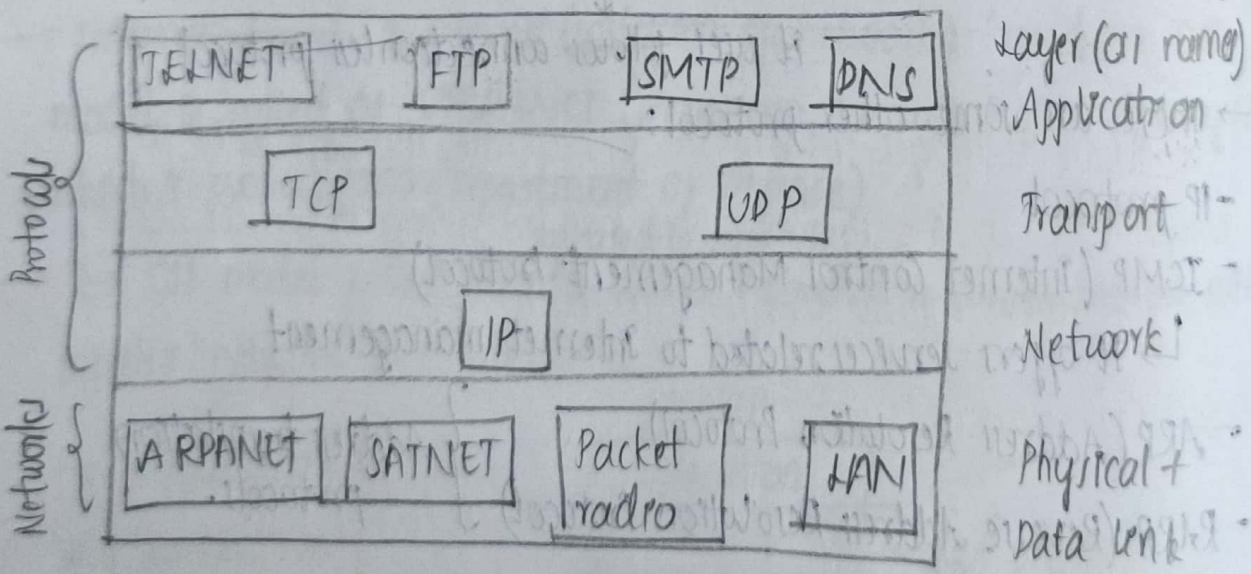
  It is a reliable, connection-oriented protocol ~~that~~ based on bytestream

  * TCP divides the message into PDU's (Protocol Data Unit). PDU is called as segment.

- UDP (User Datagram Protocol):

  It is an unreliable connectionless protocol

Fig: 1-22. Protocols and networks in the TCP/IP model initially.



(IV) Application layer:

→ It contains many protocols like:

- TELNET (Terminal Networking) (R-login or Remote login)
- FTP (File Tranfer Protocol)

- Electronic Mail (SMTP) [Simple Main Tranfer Protocol]
- DNS (Domain Name System) → Service which maps user-defined string (domain) to IP address
  - Domain → user-defined string
  - IP address → unique Id
- ~~UseNet~~ USENET (news articles)
- HTTP protcol (world wide web protocol)

Assignment-1:

1) Discuss the examples of computer networks.

Fig-1.25. ARPANET design // also include ARPANET & this fig while writing answer.

Internet (Ans)
- ARPANET, Internet Architecture
- ATM (Asynchronous Tranfer Model)
- Ethernet

* (v) **Physical layer:**

Discuss different transmission media's
SM ques

Essay type Ques

→ Transmission media are used to exchange the data among the systems/terminals.

→ Medias are divided into '2' types:
  (i) Guided transmission media (wired media)
  (ii) Unguided transmission medea (wireless based media)

→ Guided transmission media further categorised into many types:

(1) Magnetic media:- CD, ROM, harddisk kind of devices for storage -tranmit/copy data using them physical

Advantage → bandwidth is more

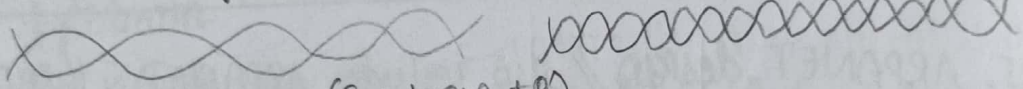
Disadvantage → speed is low

→ It uses Recordable harddisks, DVD's, ROM, etc. to carry data.

→ This media transmits more data but the transportation time may take more time (1 day or 1 week or 1 month).

(ii) Twisted Pair:

Fig-3.3: (a) Category-3 UTP (b) Category-5 UTP



(See from TB)

→ Twisted pair media - In this media a pair of wires are twisted together.

→ Twisted pair are classified into two ~~per~~ types:

- UTP (Unshielded Twisted Pairs)
- STP (Shielded Twisted Pairs) → more insulation, high quality, more costly.

→ UTP are categorised into 2 types:

(i) CAT-3 (less twists)

(ii) CAT-5 (more twists)

(category (our internet cables are CAT-3 cables)

why the cables are twisted together, what is the logic?
- Seach in Google or Chatgpt

Transmission media ---- Essay type Ques

05/08/2024 UNIT-II Monday

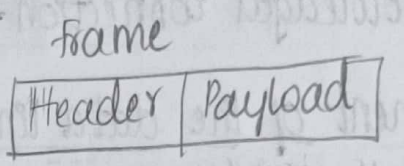
* Data Link Layer: (Second layer of osi model)

It is the protocol data Unit (PDU) is a frame.

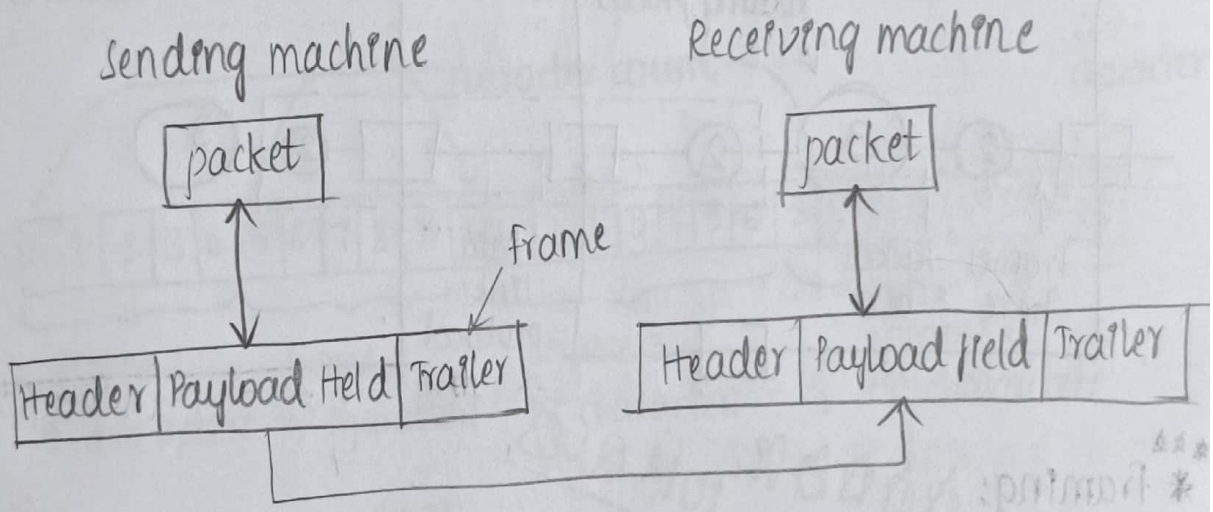
Frame → a block of bytes (or) set of bytes

Every frame has two parts:

- header
- payload



* Relationship between packet and frame:



Data link layer generates the frame using framing algorithms.

If we insert the packet directly (without modification) into the payload field then it is called as encapsulation.

If the packet is large then it is divided into set of fragments.

The process of dividing the incoming packet into multiple blocks is called framing algorithms.

2M

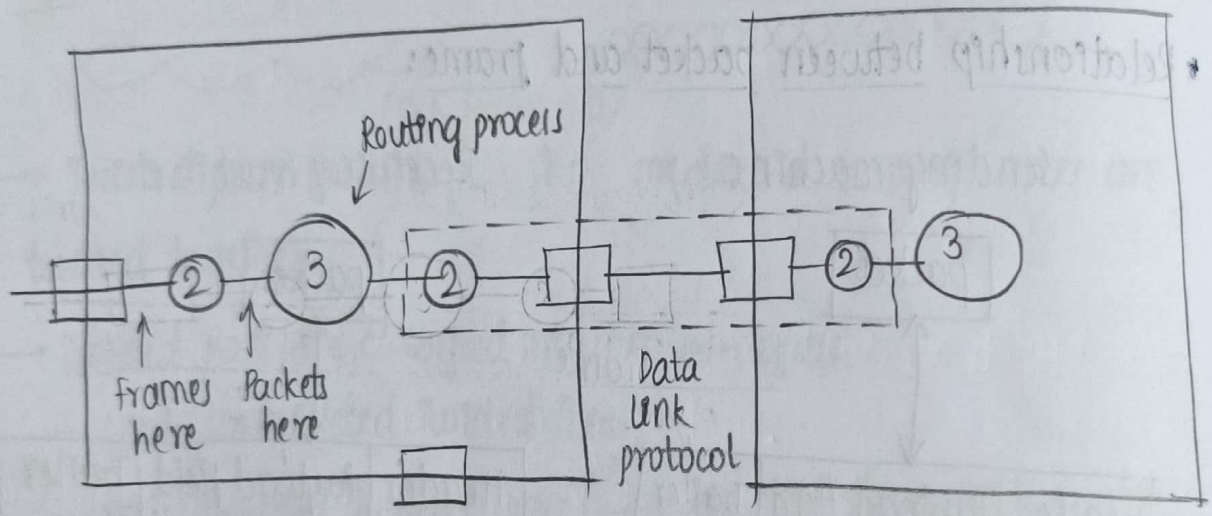
* Services provided to the network layer:

There are three types of services:

- Unacknowledged connectionless service
- Acknowledged connectionless service
- Acknowledged connection-oriented service

1M

Placement of the data link protocol: Pg: 140



***

* Framing: 8 8 8 8 8 8 10M Ques

The process of dividing the packet or a bit stream into a block of bytes is called framing algorithms.

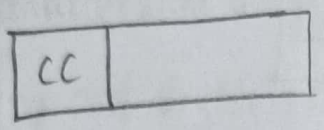
Types of framing algorithms:

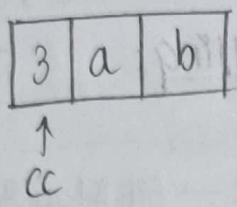
- Character count
- Starting and ending flag bytes with byte stuffing
- Starting and ending flag bits with bits stuffing
- Physical layer coding violations

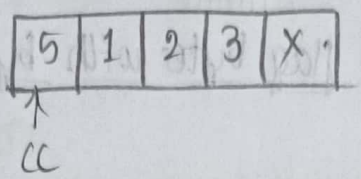
* character count:

A field in the header specify the no. of characters in a header or frame is called character count (including header)

Eg:



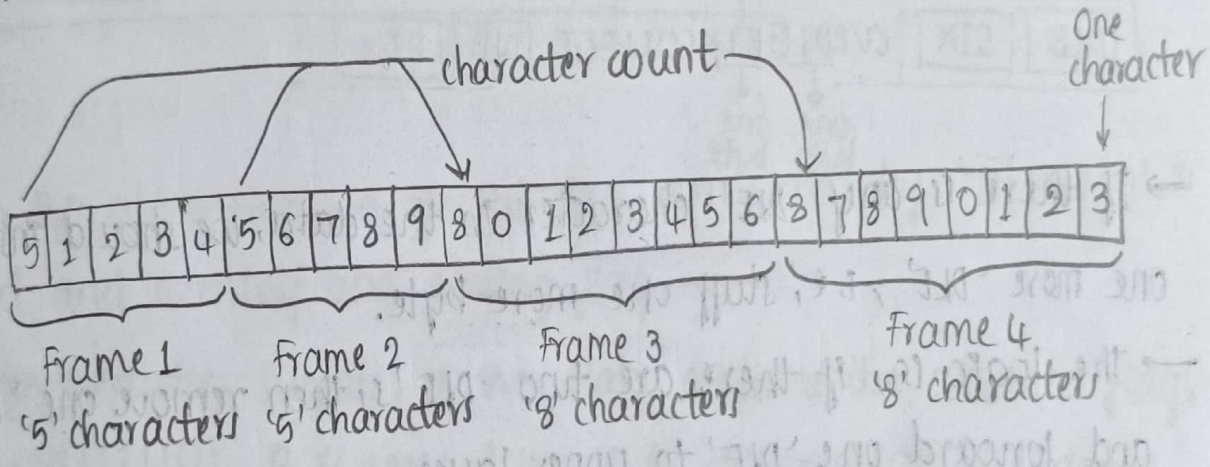




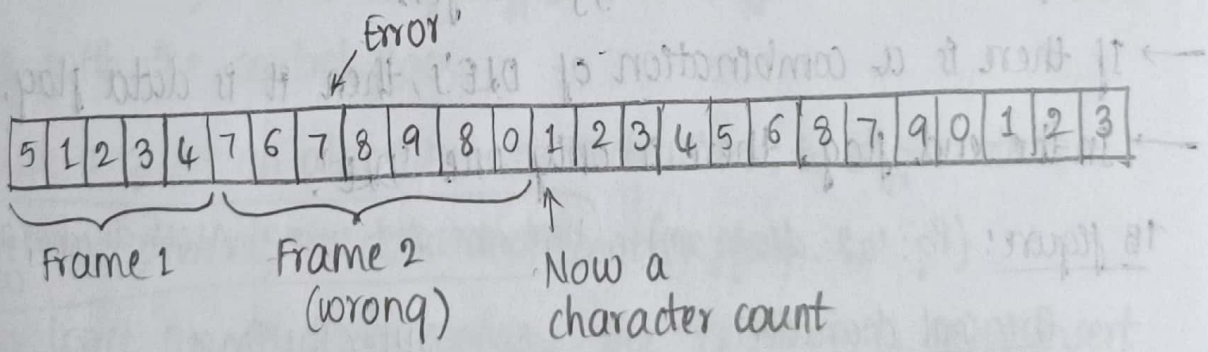
A character stream:

(a) without errors (b) with one error

(a)



(b)



In ASCII 0-31 are called non-printable and they are used for the data communication purpose.

Eg: DLE (Datalink escape) - 16

STX (Start of Text)

ETX (End of Text)

Starting byte flag is | DLE | STX |

Ending byte flag is | DLE | ETX |

Eg: | D | S | 1 | 2 | 3 | 4 | D | E |

↓ Frame

06/08/2024 Tuesday

* Starting and Ending flag bytes with byte stuffing:
* Eg: CVR

| DLE | STX | CVR | DLE | ETX |

BMP → Bit Map Protocol

Frame

| DLE | STX | CVRDLEETXCOLLEGE | DLE | ETX |

(DLE → one byte, ETX → one byte)

→ If there is any 'DLE' character in the data, we should insert one more 'DLE', i.e, stuff one more byte.

→ The logic is, if there are two 'DLE's, then remove one 'DLE' and forward one 'DLE' to upper layer.

→ If there is a combination of DLE's, then it is data flag.

→ In the end flag, there is only one 'DLE'.

TB figure: (Pg: 142 diagram)

Here, we are using ASCII as character code.

Original characters

A	FLAG	B	→ DLE ETX
A	ESC	B	→ DLE
A	ESC	FLAG	B
A	ESC	ESC	B

After stuffing

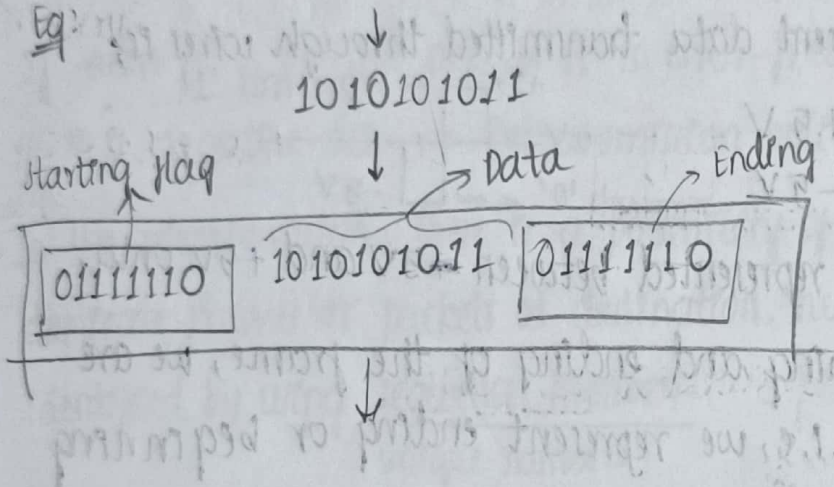
A	ESC	FLAG	B
A	ESC	ESC	B
A	ESC	ESC	ESC	FLAG	B
A	ESC	ESC	ESC	ESC	B

→ In byte stuffing, sender and receiver must have same character code.

→ Byte stuffing is not good enough or effcient. (Effcient way to differentiate two unique ~~things~~ packets is one bit ('1' or '0')).

* Starting and Ending Flag ~~byte~~ bits with bits stuffing:

Eg:



→ In this algorithm, a special flag represented by '01111110' is used and starting and ending flag.

→ ~~Unfortunately~~, Suppose, if the data contains the assumed flag, (i.e, 01111110), it is very difficult to differentiate the data flag with the control flag.

→ So, we require an algorithm or mechanism, to differentiate '01111110' present in data and control flag.

→ Our logic is, if data contains five 1's (11111), then insert a '0', next to it, i.e, we are breaking the bits sequence, i.e, we are avoiding or preventing (111110) ~~if~~ six 1's followed by '0'.

But, it is not so good logic. The good logic is if we encounter a sequence of five 1's, then if next bit is '1', then insert '0', if the next bit is '0', then ignore it. But it is difficult to implement this.

Eg: (a) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

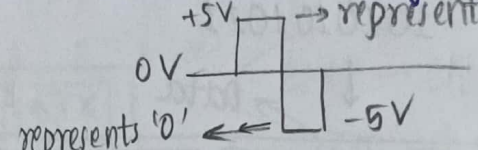
(b) 0 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 1 0 1 0 0 1 0
stuffing

(c) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0 (unstuffing)
(remove the stuffed 0's)

* Physical layer coding violation:

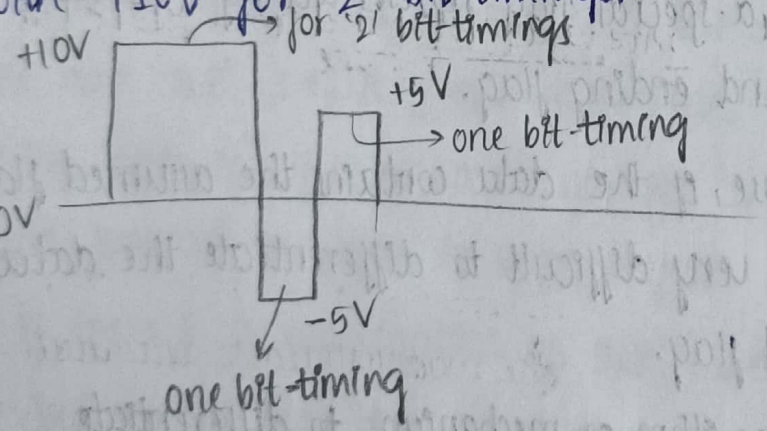
The rule to represent data transmitted through wires is;

1 ⟶ +5V
0 ⟶ −5V



The data is being represented between −5V and +5V only.

To represent beginning and ending of the frame, we are violating this rule, i.e, we represent ending or beginning with +10V for '2' bit-timings.



Bit-timing ⇒ The time upto which the voltage is raised/lowered to represent one bit (1/0).

09/08/2024 Friday

* Error control: → IM (what is it, what are algorithms in it)

Errors occurred when transmitting data from source to destination

→ It deals with transmission errors.

→ Error control has two modules:

- Error detection
- Error correction

Error correction ~~has two~~ is divided into two mechanisms:
- Error correction by destination itself (self-healing solution)
- Error correction by the feedback from the destination to the source. (Retransmission policy is used. Feedback can be in the form of acknowledgment).

acknowledgment may be < Positive (no error)
Negative (there is error)

If ~~ackn~~ it is positive ack. ⇒ it is error-free

If it is negative ack. ⇒ Retransmission policy is used

Case(i):
- In the retransmission, there is a possibility of ~~du~~ arrival of duplicate frames or packets at destination. These duplicates are identified by using sequence numbers.
(unique numbers)

RTT ⇒ Round Trip Time → worst case time required to transmit data from source to destination and receive feedback/ack. from destination to source.

Case(ii):
- Suppose if the acknowledgment itself is damaged/destroyed/corrupted, the source may be at infinite state. To avoid this situation, we introduced a concept called as timer. Timer will start for every specific frame with RTT value. (If RTT time is reached, i.e, timeout, the retransmission is automated.)
- If any data link layer, a protocol which uses ack., retransmission, sequence numbers and timer is called ARQ (Automatic Repeat Request) protocol.

* Flow control: IM → what is it
→ what are algorithms in it

→ It deals with regulating data flow rate b/w two different speeds of terminals.
→ It has two different approaches:
- Feedback based flow control (Stop & wait protocol)
- rate (data rate)-based flow control (~~Negot~~ Flow Negotiation protocol)

* Error detection:

- Transmission errors are of two types: single line
  - Single-bit errors (they occur in serial communication)
  - Multi-bit errors (they occur in parallel communication) multiple lines

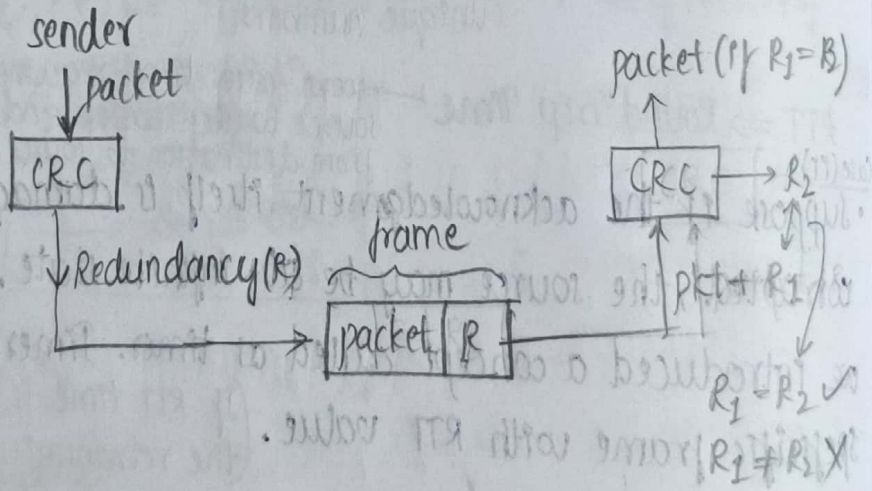
→ Errors are detected by using exclusive OR operation. The original string and received string are compared. If result is zero, then there are no errors, else there are errors. comparision by using

eg: 10001001
    11001000

    01000001

    ≠ zero ⇒ error-prone

- Error detection has two modules:
  - Sender
  - CRC



- CRC (Cyclic Redundancy Checkport):

It is an algorithm used to derive a compressed duplicate copy called as Redundancy (R) for original data frame or packet.

10/08/2024 Saturday

* CRC Algorithm/- Sender:

Step-1: Let D(x) be a data load from the network layer.

Step-2: The given generator function (agreed by source and destination), G(x).

Step-3: find the length of the generator function (the binary string length) say 'l'.

Step-4: Append (l-1) binary zeroes to the data word D(x). (D(x)+(l-1) zeroes (auxiliary codeword))

Step-5: Implement/Start arithmetic binary division operation (CRC algorithm).

Step-6: By the end of the division, we will get a remainder that is called a "Redundancy" - R(x)

Step-7: The final transmitted PDU (Protocol Data Unit) is codeword - C(X) = D(X) + R(x)

* CRC Algorithm - Receiver Routine: Essay type

Step-1: The received codeword is C(x).

Step-2: Already the agreed/committed generator function with the source is G(x).

Step-3: Apply the arithmetic binary division, G(x) as the divisor and C(x) as the dividend.

Step-4: By the end of the division operation, you will get a remainder - S(x) [Syndrome]

Step-5: If the syndrome S(x) = 0, then there is no error in the received data C(x). If S(x) is non-zero, then there is an error in the codeword C(x).

NOTE: Here, arithmetic binary division is Modulo-2 division. ⇓ XOR operation

Eg: $D(x) = 1010111$

$G(x) = 1011$

Append (4-1=)'3' zeroes to $D(x)$.

$1010111000 \Rightarrow$ auxiliary codeword

```
1011 ) 1 0 1 0 1 1 1 0 0 0 (
       1 0 1 1
       -------
       0 0 0 1 1 1 1
           1 0 1 1
           -------
           0 1 0 0 0
             1 0 1 1
             -------
             0 0 1 1 0 0
               1 0 1 1
               -------
               0 1 1 1
```

$R(x)$

Codeword is $C(x) = \underbrace{1010111}_{D(x)}\underbrace{111}_{R(x)}$

Receiver routine: Case(1):

```
1011 ) 1 0 1 0 1 1 1 1 1 (
       1 0 1 1
       -------
       0 0 0 1 1 1 1
           1 0 1 1
           -------
           0 1 0 0 1
             1 0 1 1
             -------
             0 0 1 0 1 1
               1 0 1 1
               -------
               0 0 0 0
```

$0000 \Rightarrow S(x)$

$\therefore$ The codeword received is correct.

Case(ii): Suppose, one of the bit is inverted (changed from '0' to '1' (or) '1' to '0') in the codeword, prove that there is an error in the received data.

The actual codeword is 1010111111.

According to question, let us assume that the received codeword is 1000111111 (higher order 3rd bit is inverted).

```
1011) 1000111111 (
      1011
      ----
       001111
         1011
         ----
          01001
            1011
            ----
           001011
             1011
             ----
            00001  → S(x)
```

∴ The codeword received has errors.

12/08/2024 Monday

*Polynomial CRC:

- The conversion from polynomial to the benary:

Eg: $x^6 + x^5 + x^3 + x^2 + 1$

$\Rightarrow 1.x^6 + 1.x^5 + 0.x^4 + 1.x^3 + 1.x^2 + 0.x^1 + 1.x^0$

1 1 0 1 1 0 1

∴ $x^6 + x^5 + x^3 + x^2 + 1 \Rightarrow 1101101$

- Conversion from binary to polynomial:

Eg: 1010111

1 0 1 0 1 1 1
$2^6\ 2^5\ 2^4\ 2^3\ 2^2\ 2^1\ 2^0$
$x^6\ x^5\ x^4\ x^3\ x^2\ x^1\ x^0$

$\Rightarrow 1.x^6 + 0.x^5 + 1.x^4 + 0.x^3 + 1.x^2 + 1.x^1 + 1.x^0$

$\Rightarrow x^6 + x^4 + x^2 + x^1 + 1$

$\therefore 1010111 \Rightarrow x^6 + x^4 + x^2 + x^1 + 1$

link

* Elementary data link layer protocols:

- Data ~~link~~ link layer protocols are divided into two categories:
  - Data link layer protocols for noiseless channels
  - Data link layer protocols for noisy channels

* Data link layer protocols for noiseless channels:

~~Assumptions:~~ Network model assumptions:

- There are n no. of stations/terminals
- Each station has a data ready to transmit
- Similarly, every terminal is ready to receive
- The communication medium is error free.
- Every machine has infinite buffer
- Systems are high-end terminals (every system is at equal speed)

* Simplex Unrestricted Protocol:

short ans

eg: FM Radio.

The first protocol is called Simplex Unrestricted Protocol

(Simplex = one-way data transfer (Design issues of layers and physical layer - it was discussed here)

→ In this (simplex) protocol, data is transferred in one-way.

→ Simplex means one-way data ~~transfe~~ transmission, the data is transmitted from source to destination.

→ Unrestricted means there are no more restrictions in terms of processing, buffers (memory), transmission errors (no errors).

• So, in this protocol, a sender gets the packet from the network layer as a packet and generates the frame, then forwards it ~~to the~~ as a stream of raw bits to the physical layer. Whereas, the receiver fetches the bits stream from the physical layer, recognises the frame and then forward the data to the network layer as a packet.

Read these codes from T.B

Sender program:

```
{  packet
   ~~plot~~ Buffer;
   frame f
   while(1)
   {
      From_Network_Layer(&Buffer);
      f.info = Buffer
      To_Physical_Layer(f);
   }
}
```

frame

Header	Payload

info

f.info

Receiver program:

```
{  frame s;
   while(1)
   {
      wait_for_event();
      from_Physical_Layer(&s);
      To_Network_layer(s.info);
   }
}
```

→ It pushes data into communication medium and invokes this event

Frame arrival event

13/08/2024 Tuesday

This kind of protocol is called an imaginary or unrealistic protocol and called as "utopia".

- As it is an unrealistic protocol, to design a realistic protocol, we are violating one assumption, i.e, "there are different speeds of terminals exist."
- So, in the next protocol, we are going to introduce flow control.

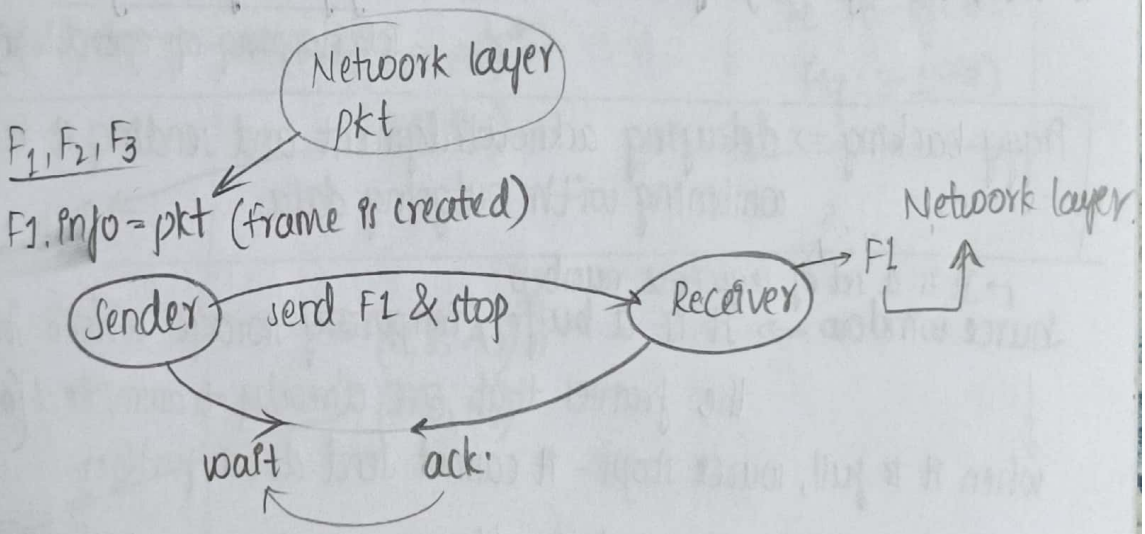
* Simplex Stop-and-Wait Protocol: → short ans

- ~~In th~~ Still it is a simplex protocol, i.e, one-way — sender sends the data and receiver receives the data.
- It is an error free communication medium, i.e, noiseless channel.
- It has finite buffers and finite processing speed.
- Since, the systems have different speeds, we must include flow control module in our protocol.

Program: (Pg: 155)

```
typedef enum {frame_arrival} event_type;
#include "protocol.h"
void sender2(void)
{
    frame s;
    packet buffer;
    event_type event;
    while(true)
    {
        from_network_layer(&buffer);
        s.info = buffer;
        to_physical_layer(&s);
        wait_for_event(&event);
    }
}
```

```
void receiver2(void)
{
  frame r,s;
  event_type event;
  while(true)
  {
    wait_for_event(&event);
    from_physical_layer(&r);
    to_network_layer(&r.info);
    to_physical_layer(&s);
  }
}
```



* Data link layer protocols for Noisy channels:

* Simplex protocol for noisy channel:

- It is still one-way but it is along unreliable channel (there may be data loss).
- In this protocol, we required error control module.
  - -ve & +ve ack.
  - Retransmission
  - Sequence numbers (duplicates are identified)
  - Time control (to avoid infinite waiting)

20/08/2024 ★★★★★ (5-star question) → Essay type Tuesday

~~One-bit~~ sliding window protocol:

There are two types:

(i) 1-bit sliding window protocol

(ii) n-bit sliding window protocol (n-bits are used in sequence numbers)

Receiver window and sender window need not be same size (their size may be based on their speeds)

Issues with previous protocol / Assumptions:

→ Previous protocols are one-way, but the user expected two-way communication.

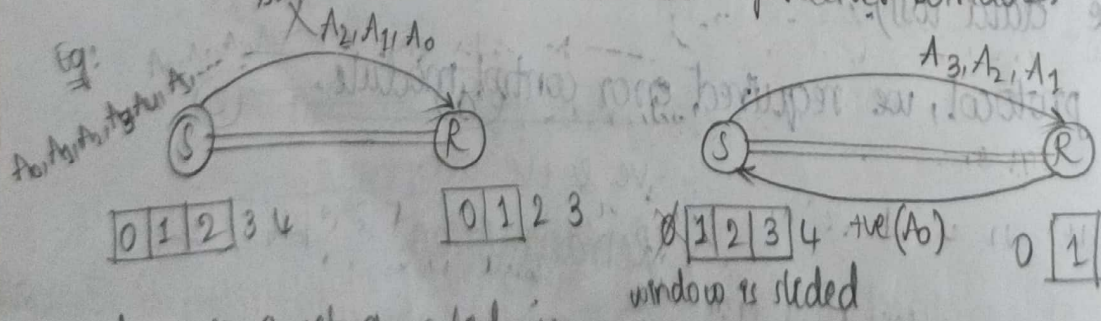
→ As the previous protocols performance is less/resource utilization is less, to improve performance, we use pipeling concept. (overlapping of operations)

Piggy backing ⇒ delaying acknowledgment and sending it by combining with outgoing data

Source window ⇒ It is a set of sequence numbers
It is a buffer/temporary storage which stores the frames that are already transmitted (outstanding frames)
when it is full, source stops - it cannot send data further

Receiver window ⇒ It is a buffer/temporary storage which stores the frames that are received

- When these windows are full, then the window slides to next sequence number ← to be transmitted sequence no. in case of src window. to be received in case of receiver window.



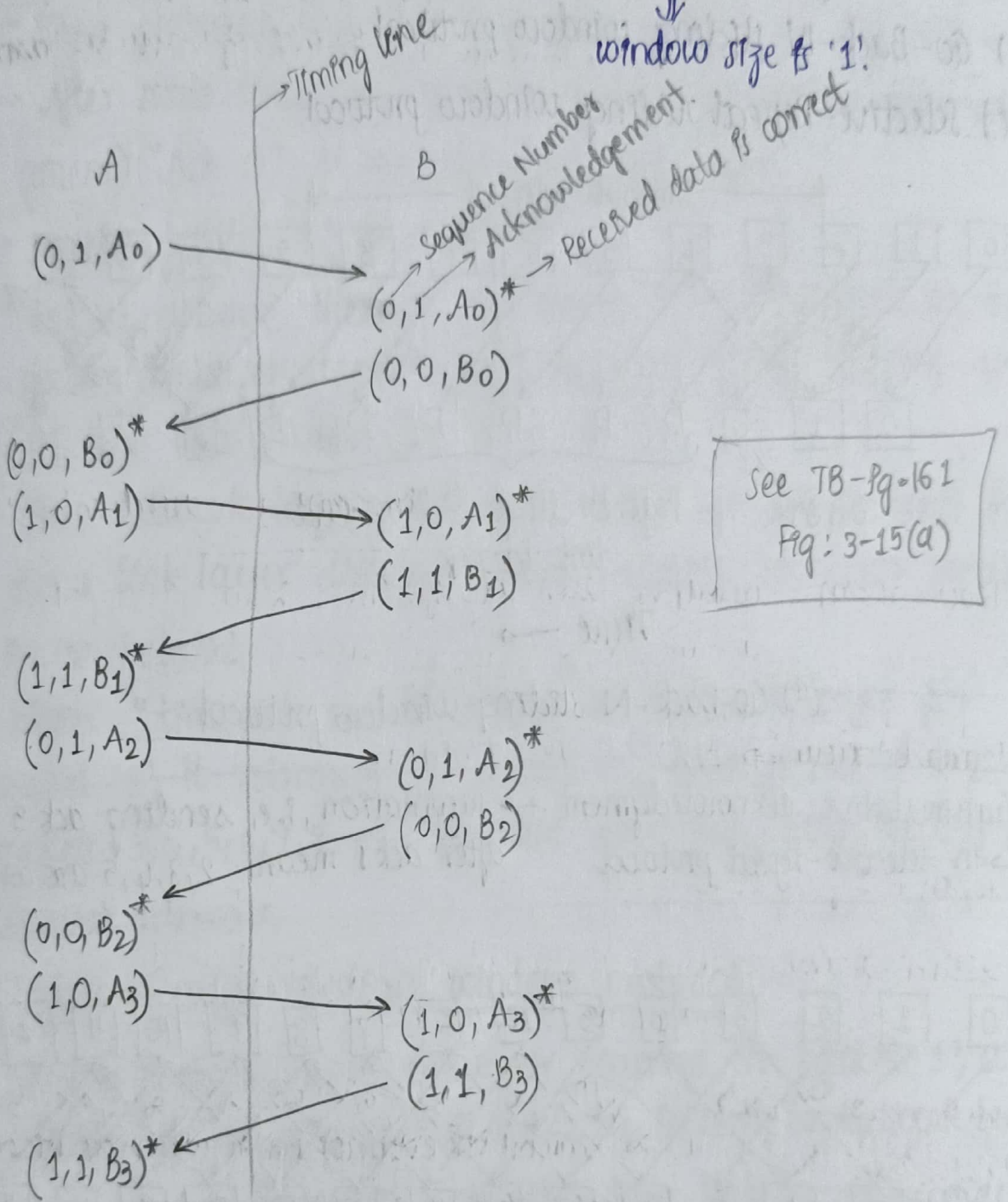
window is a set of valid sequence numbers. let us assume src window with sequence numbers 0,1,2,3,4,... of size '3'. when it receives +ve ack, then the window slides to next sequence no., i.e, 1|2|3. similarly, sliding takes place in receiver window also.

* 1-bit sliding window protocol: Pg-161, Pfq: 3-15(a)

→ 1-bit ⇒ 1-bit sequence number ⇒ either '0' or '1'

⇓

window size is '1'.



See TB-Pg-161
Pfq: 3-15(a)

'A' sends frame (0, 1, A0). → Data Field

sequence No. Acknowledgment field

'B' receives it and sends (0, 0, B0) → data to be sent by 'B'

sequence No. Ack.

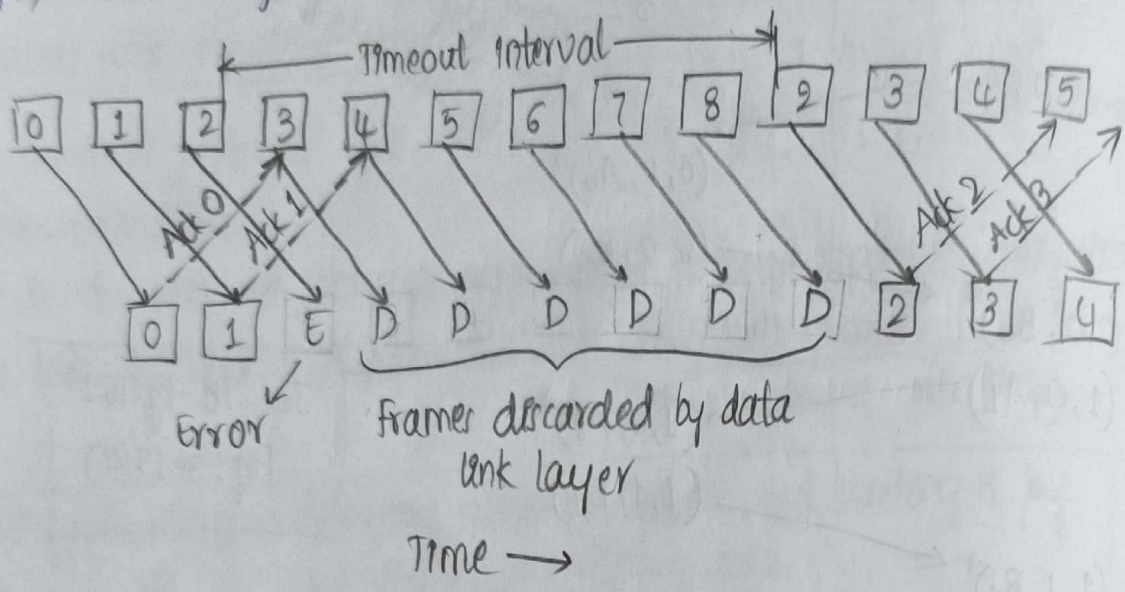
⇓

sequence no. of frame sent by 'A'

08/2024 Thursday

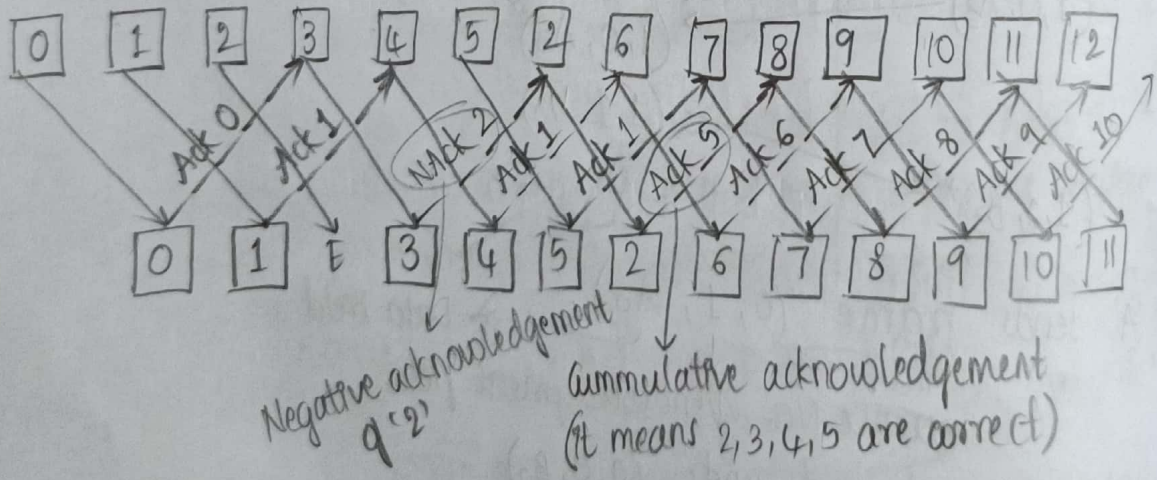
* n-bit sliding window protocol:

- n-bit sliding window protocol has '2' types of algorithms:
  (1) Go-Back-N sliding window protocol
  (2) Selective-Repeat sliding window protocol



(a) Go-back-N sliding window protocol

> Cummulative acknowledgment → summation, i.e, sending ack 5 after ack 1 means 2,3,4,5 are correct.
> ↳ in selective-repeat protocol



(b) Selective-Repeat sliding window protocol

Go-Back-N sliding window protocol:

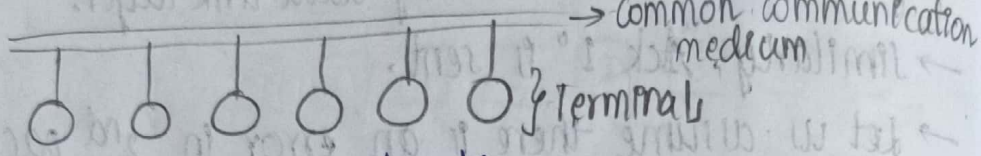
→ First 0th packet is sent to the data link layer.
→ Then followed by packets numbers 1,2,--- are sent.
→ After some time an acknowledgement (positive acknowledgment) "Ack 0" is sent by data link layer.
→ Similarly, "Ack 1" is sent.
→ Let us assume there is an error in 2nd packet. So, the data link layer doesn't send any ack. (This is like -ve ack. in this protocol).
→ The network layer sends packets 3,4,5,6,7,8, but the data link layer discards them because an error occurred in packet '2'.
→ When "timeout event" occurs in network layer for packet '2', it retransmits packet '2', then followed by packets 3,4,5,6,7,8,--- because even they also reach their respective timeout intervals.

Selective-Repeat sliding window protocol:

→ In this protocol, when an error occurred in packet '2', a negative acknowledgement "NAck 2" is sent to network layer.
→ So, the packets received until the data link layer receives packet '2', i.e, packets 3,4,5 are stored in a buffer.
→ When packet '2' is received again, a cummulative acknowledgement 'Ack 5' is sent to network layer, which means the packets (received by Ack 1) 2,3,4,5 are correct.
→ Then the remaining packets are received and ack's are sent similarly (and packets 2,3,4,5 are arranged in order based on their sequence numbers).

* Medium Access ~~Protocol~~ Control (MAC)/Multiple Access Control:

• In broadcast transmission technology networks, there is a single common shared communication medium used by many terminals equally.



• In the broadcast ~~network systems~~ networks if ~~more than one system~~ two or more systems simultaneously ~~communicate~~ transmit data, then there is overlapping of signals and that event is called collision.

23/03/2024 Friday

* Dynamic Channel Allocation methods:

• Network assumptions:

- N-stations
- Single communication channel
- Collision (only one type of error in this network) (write def. in exam)

• Time assumptions:

The time at which we access the media. There are two types:

- Continuous → access at any time (→ like restaurant)
- Slotted → access is allowed only in the beginning of slot (→ like theatre)

• (a) Carrier sense:

→ Before, channel transmits the data, it will sense whether the communication channel is empty or occupied.

(if empty it transmits)

(b) No carrier sense:

(else we will wait)

* 1st Algorithm:

* ALOHA: long ans

Random Access Protocols / Essay type

Collision free protocols

ALOHA
CSMA
CSMA/CD

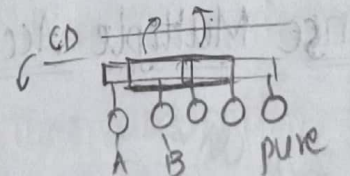
Assumptions:

- N-stations
- Single common communication channel
- Collision
- (a) Pure ALOHA (continuous)
  (b) Slotted ALOHA (slotted)
- No carrier sense

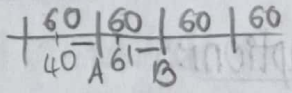
If 'A' transmits '10' bits of data into channel and then at 9th bit 'B' started transmitting the data, in this case, last bit of 'A' and 1st bit of 'B' collides, which is detected by collision detection algorithm.

CD generates two random numbers for 'A' and 'B'. 'A' will access medium/channel at the time allocated to it and 'B' will retransmit the data at the the time allocated to it.

If 'A' got 40
'B' got 61



slotted



then 'B' waits 21 sec in pure ALOHA. If it is slotted, then it will wait for the beginning of next slot, i.e, 'A' waits for 20 sec and 'B' waits for 59 sec.

↳ as next slot begins at 60

↳ as next slot begins at 120

* Channel Allocation Methods:

A method which allocates a common single channel to multiple terminals without collision:

There are two types:

(i) Static
(ii) Dynamic

- In static allocation whole channel is divided into multiple sub-channels.

There are again two types:

(i) • FDMA (Frequency Division Multiple Access)
Eg: Antenna dish
The whole frequency channel is divided into multiple frequency sub-channels.

(ii) • TDMAC (Time Division Multiple Access)
In TDMA, operating time divides into multiple slots.

(iii) •
In dynamic, there is no division

24/08/2024 Algorithm/ Saturday

* 2nd Protocol - Carrier Sense Multiple Access (CSMA) Protocol:

long ans

Assumptions:

- N-station model
- Single channel
- Collision
- ~~no car~~ Carrier Sense

In CSMA protocol, a mechanism is called as carrier sense. ~~Other transmit~~ Before transmitting the data, the channel is sensed first to check whether it is free or busy. If the channel

is busy, then the terminal can wait for the resource in two ways:

(i) continuous waiting ⇒ Persistent-CSMA protocol

↳ the terminal will wait continuously until the channel is free, and once it is free, the resource is allocated to this terminal / this terminal get the channel.

(ii) Non-persistent CSMA protocol

↳ The terminal will perform context-switching and it performs another task. So, eventhough the channel becomes free, it cannot acces the channel because it is performing another task.

Time assumption:

→ If time assumption is continuous, then it is called 1-persistent CSMA protocol.

↓

Probability = 1

↳ probability that our current waiting terminal (rated terminal) get the channel when it is released by other terminal's is 1.

→ If it is slotted time assumption, then it is called p-persistent CSMA protocol.

↓

Probability varies because based on the time slot in which the channel is released, the probability ranges from 0-1.

to acces it

* 3rd Algorithm – CSMA/CD Protocol:

- To improve the efficiency of CSMA, another algorithm or protocol called as CSMA/CD protocol is introduced.
- In this protocol, instead of invoking the collision detection algorithm after each frame, we invoke it at bit-level (i.e, after every bit is transmitted) and if collision is detected, then, the remaining data transmission is stopped.

* Collision Free Protocols:

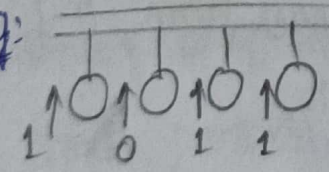
- In collision free protocols, we require an agreement or agreement information to accell the channel.

I. Bit-Map Protocol:

→ Mapping a bit to each terminal.

- In this protocol, one bit is mapped to each terminal. If the terminal is interested to transmit data, then, it sends '1', else, it sends '0'. (In given time → bit-timing)
- All the terminals receive this sequence of bits (So, all the terminals have same agreement now), then based on this sequence, the data is transmitted into channel.

Eg:



→ In '4' bit-timings, all four terminals will transmit either '1' or '0'.

1011 ---data---

It means terminals 1, 3, 4 are interested in transmitting data, while terminal '2'

II. Binary countdown Protocol:

- In previous protocol, as no. of terminals increase, the no. of bits also increase which is not a feasible solution. So, we have this next protocol - Binary countdown.

27/08/2024 Tuesday

→ We allocate binary addresses to each terminal.

> When we are fetching/processing data in any hardware using microprocessor, then we decide whether to start from right or left / lower-order bits or higher-order bits using ~~ie~~

→ Initially, at 0th ~~bit~~-timing, all the ~~calling~~ terminals which are interested in transmitting data, broadcast their LSB into the communication channel and their resultant is obtained. If the resultant bit is '1', then the terminals with their LSB as '0' drop. of the remaining terminals

→ In next bit timing, the next bits is broadcasted into the communication channel and resultant bit is obtained. Again if it '1', then the terminals with corresponding 2nd bit as '0' are dropped and this proces continues until all the terminals transmit data.

* Ethernet:

short ans & Essay type

- → It is a LAN standard → flavors, cabling, frame structure
- → IEEE802.3 (Ethernet)
  - It uses 1-persistent CSMA/CD protocol

* Ethernet cabling:

- Ethernet cabling contains 4 cables

Fig: The most common kinds of Ethernet cabling

Name	Cable	Max. seg.	Node/seg.	Advantages
10Base5 (500 m)	Thick coax	500 m	100	Original cable; now obsolete
10Base2 (200 m)	Thin coax	185 m	30	No hub needed
10Base-T (twisted-pair)	Twisted pair	100 m	1024	Cheapest system
10Base-F (Fiber optics)	Fiber optics	2000 m	1024	Best between buildings

10Base5: 10 Mbps = it specifies speed; Base-band signalling = Digital signalling

F = it specifies length and type of cable

Amplifier → regenerates signals to a proper value.
(low signals to high signals)

Repeater → It is the device which is used to connect the (cabling, data encoding technique, frame format)

UNIT - III: (Syllabus for mid-I) store & forward technology, Ethernet
Optimality principle

Design issues of network layer, routing algorithms - static routing algorithms (shortest path routing algorithms), Dynamic routing algorithms (Distance vector routing algorithm, Link state routing algorithm), Multi-cast routing algorithms, Broadcast routing algorithms.

10 M → distance vector
difference b/w datagram & shortest path algorithms

1M → optimality principles
routing algorithms < what is it types

30/08/2024 Friday

UNIT-III

* Routing Algorithms:

Leading concept ⇒ permanent routing
↳ all the routes are stored in routing table

Session ⇒ when connection is established, then routes are stored in routing table and are deleted after establishment is removed.

Every Routing consists too details ← routing table

Forwarding ⇒

We use it when there is dynamic topology ← Routing tables are not permanent, it is updated periodically

Adaptive algorithms ⇒ dynamic routing algorithms
↳ According to conditions of network, routing tables and routing details are updated periodically
Using some process, all routing details are monitored,

Non-adaptive algorithms ⇒ static routing algorithms
↳ when network is started, then routing table is established based on the topology and it is permanent.

Optimality Principle: (1 Mark)
(from TB)

(10M) → optimum with respect to metric

* Shortest Path Routing:

→ It is a static routing algorithm.

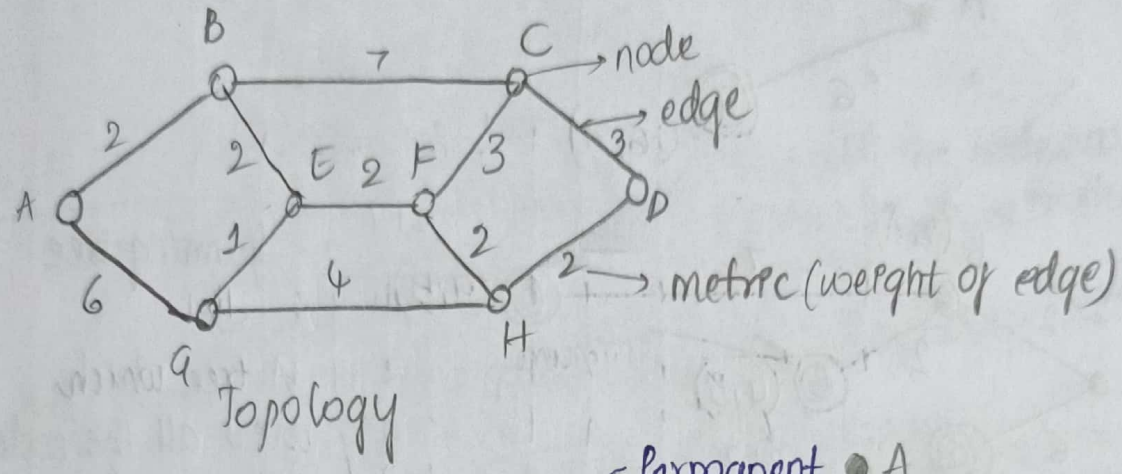
terminals ⇒ nodes

transmission lines ⇒ edges

Graph ⇒ call it as topology in CN
↳ the way the terminals are connected.

→ The metric (weight of the edge) can be physical distance b/w

two node or it can be a bandwidth or it can be delay ~~or~~ in transmission time or combination of above.



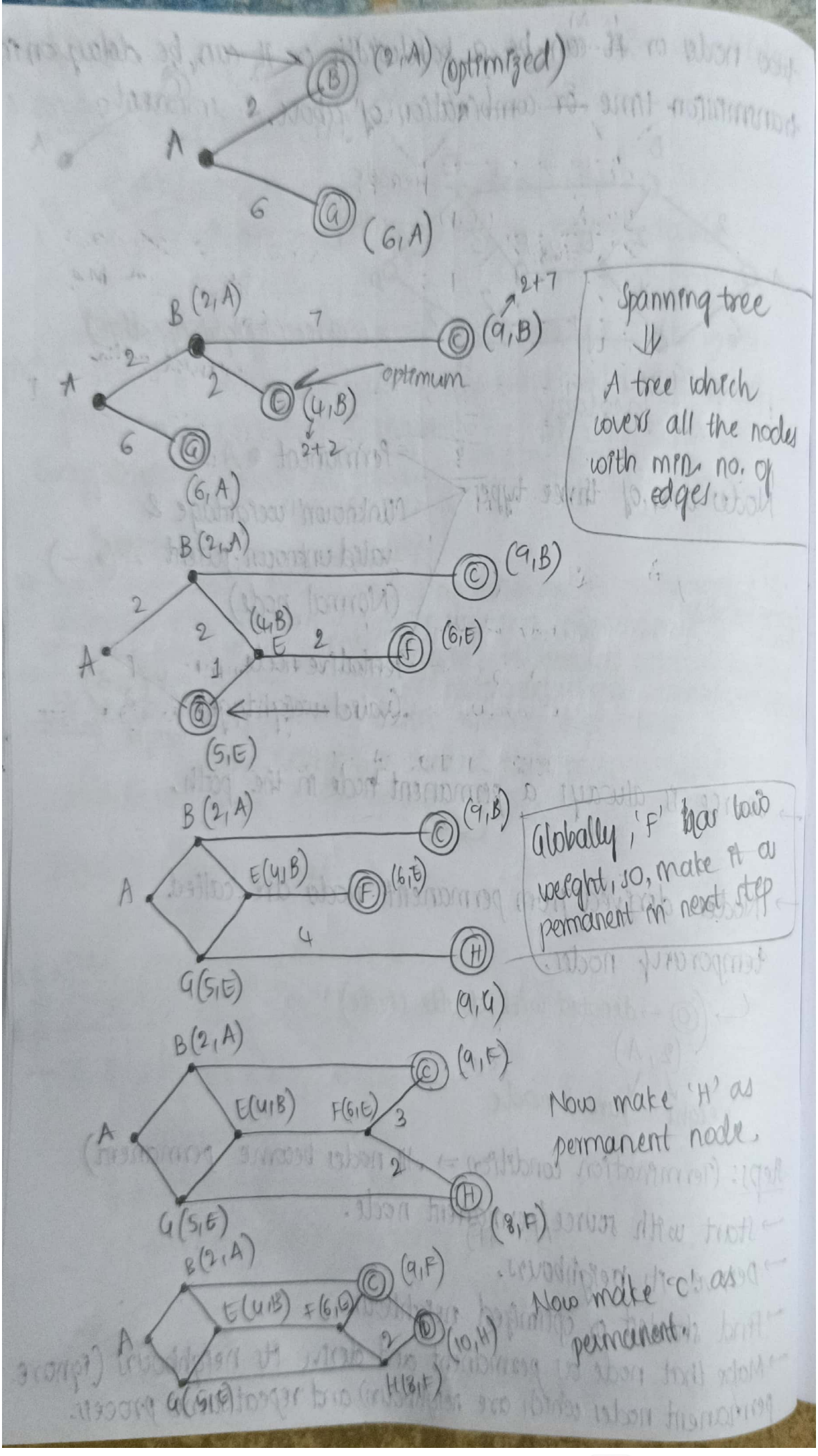
Topology

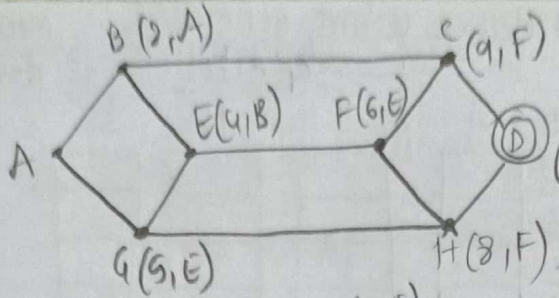
Nodes are of three types
- Permanent ● A
- Unknown weightage & ~~valed~~ unknown parent A (●, –) (Normal node)
- Tentative node (valed weightage) A (2, B) (2 → weight, B → parent)

→ Source is always a permanent node in the path.
↳ (●)

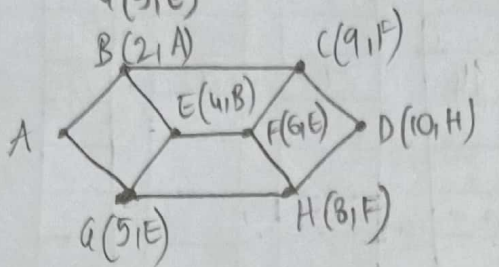
→ Nodes derived from permanent node are called temporary nodes.
↳ (◎ → denoted with double circle)
(2, A)
weight, parent node

Steps: (Termination condition ⇒ All nodes become permanent)
→ Start with source/permanent node.
→ Derive its neighbours.
→ Find shortest or optimized neighbour.
→ Make that node as permanent and derive its neighbours (ignore permanent nodes which are neighbours) and repeat same process.





Now make 'D' as permanent.



Now all the nodes are permanent, so exit the algorithm.

Path from 'A' to 'D' ⇒ A-B-E-F-H-D ⇒ optimal path
Path from 'A' to 'E' ⇒ A-E
Illy A-B-E, A-F, A-B-E-F → This is present in optimal path. This is known as optimality principle

An optimal is a collection of optimal paths.

Optimality Principle ⇒ If 'I take 'q' is source and 'k' is destination
(or) If we derive a path from 'q' to 'k' and consider an intermediate terminal 'j' and the path from 'q' to 'j' falls on the same path as that of 'q' to 'k'.

Saturday

31/08/2024

* Distance vector routing protocol/algorithm:

→ To know changing dynamics in a network, we use "sharing".

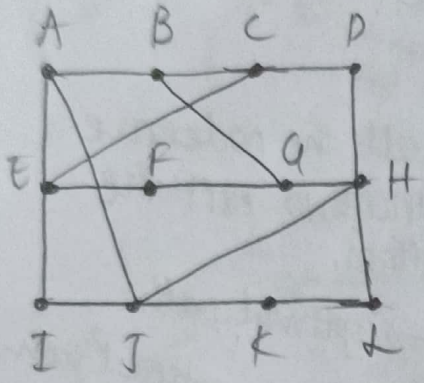
what you are sharing — sharing → to whom you are sharing

2 principles:

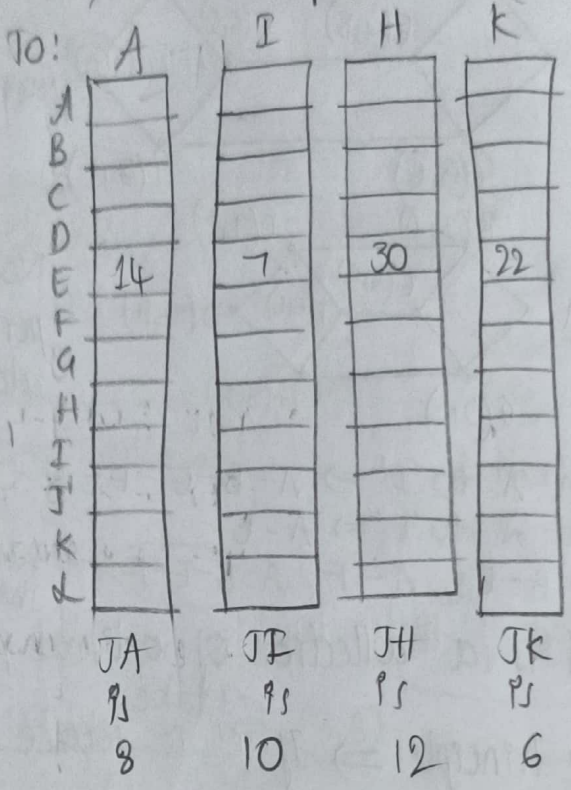
⇒ Neighbour info → sharing → to all terminals
⇒ All info → sharing → to neighbour

Based on above two principles, we have two ~~protocols~~ algorithms

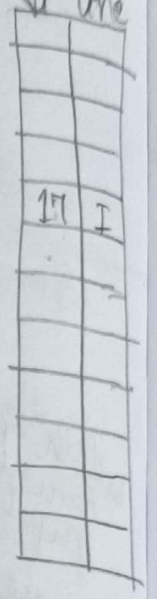
Fig: 5-9 TB pg no: 271



distance vectors generated by A, I, H, K

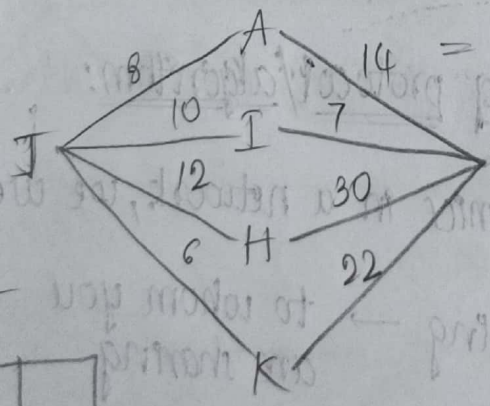


New estimated delay from J here



→ Every neighbour generates distance vector packets.

→ Based on all the received distance vector packets, we can generenerate resultant vector for 'J'.



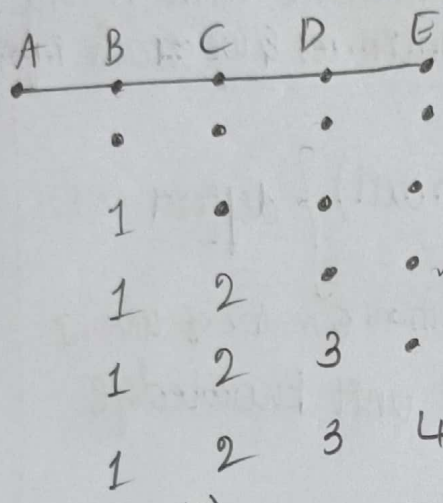
J

A		
B		
C		
D		
E	I	17

Write this explanation how you got these values step-by-step in exam

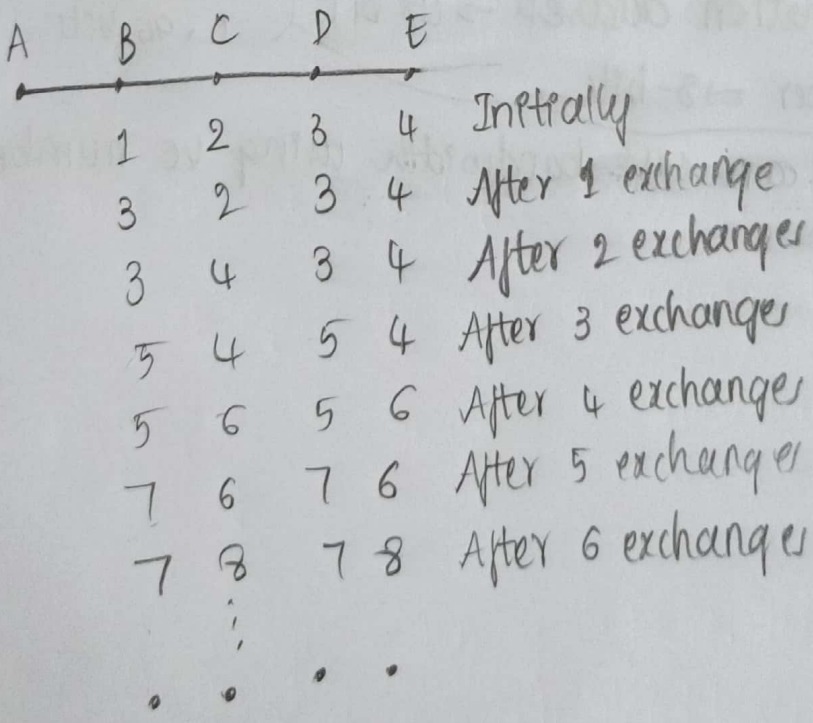
* count to infinity problem :

hop-count ⇒ It is one of metric count which represents how many jumps are made.



(a)

Initially, 'A' transmit data to 'B' in one jum or hop, so after one exchange we wrote '1' under 'B'. Then, 'B' tranmits data both to 'A' and 'C' (as they are its neighbours). Now, if 'C' wants to tranmit data to 'A' it should transmit to 'B' & then 'A' so hop-count is '2' and this process continues.



(b)

Initially, 'A' transmits data to 'B'. Then let us assume the path/connection b/w 'A' & 'B' is destroyed, then 'B' transmits data

to 'C' and C's hop-count became '2'. Now, as 'B' doesn't have direct connection with 'A', it assumes that it can communicate with 'A' via 'C' whose hop-count is '2' (which means 'C' can transmit data to 'A' in '2' jumps or hops). So, B's hop-count becomes '3' now. Now 'C' assumes it can communicate with 'A' via 'B' & it's hop-count becomes '4' & this process continues & we reach infinity.

Pg-263

Connection-oriented (virtual circuit) } differences
Connectionless (datagram)
→ before table write definitions & matter of unit-I
table

draw it & explain using 1st unit knowledge

10M Ques

VC number ⇒ Virtual circuit number
↳ when connection is established, this no. is assigned

Full destination address → 48 bits (Source + destination ↳ 96 bits)
VC number ⇒ 8-bit

↳ So we can save bandwidth using VC number