Page NO.

1. 1 to 61 – Mid Term
2. 62 to 110- Final Term

MD IFTAKHAR KABIR SAKUR

25th BATCH

COMPUTER AND COMMUNICATION ENGINEERING

International Islamic University Chittagong

COURSE CODE: CCE-4701

COURSE TITLE: Data Communication and Computer Networking

COURSE TEACHER:

Md. Humayun Kabir

Lecturer
Computer and Communication Engineering

CCE-4701

Data Com. & Computer Networking

Data & Information:-

- Data raw facts that are collected (publishing, result)
- Information is processed data that helps us to take decision (The result of mine).

Data Network:-

→ A system designed to transfer data from one access points to another access points, via data & switching, transmission lines, and system controls.

→ DN consist of communication systems (Circuit switching, leased lines, packet switching networks)

Data Communication

→ DC is the process of using computing & communication technologies to transfer data from one place to another, or between participating parties.

→ Data communications is transmission of digital data among two or more computers.

And a Computer Networks or data networks is a telecom network that allows computers to exchange data.

→ This network is built using wire or wireless.

The best computer Network is internet.

⇒ A Network of Computers is called as autonomous Computers.

Autonomous means no Computer can start, stop or control another Computers.

⇒ This Data processing system is made up of hardware & software.

Characteristic of Data Communication:-

① Delivery:- Data should be delivered in the correct destination & correct user.

② Accuracy:- Should deliver data accurately without any errors. The data may get corrupted during transmission affecting the accuracy of the delivered data.

③ Timeliness:- Audio & video data has to be delivered in a timely manner without any

delay. Such a data delivery is called real time transmission of data.

Jitter:- variation in the packet arrival time. Uneven jitter may affect the timeliness of data being transmitted.

Components of Data Communication

5 Components:-

1] Sender / Transmitter:-

-> Simple device that can send a message
-> It can be computer, smartphone, walkie-talkie,

2] Receiver:-

-> The device which receives a data.
-> Device which is capable of receiving data.
-> For example:- Computer, mobile, smartphone, TV. etc.

3] Message:-

-> A piece of information
-> Sends from sender to receiver
-> Text, number, image, audio, video etc.

Transmission Medium / Communication Channels:-

→ Through which messages are passed

→ Can be wired or wireless.

→ Connects two or more stations.

→ Example:- TV Cable, Telephone Cable, Ethernet Cable, Microwave etc

Protocol:-

→ Set of rules. followed by sender & receiver to communicate data.

→ Without this it feels likes two person trying to talk in different language.

→ When sending datas it should be known to receiver too or it would be meaningless.

Aut-22 1(b)

Protocol & Functions

1] Data Sequencing:- Log message to divide করে packed আকারে Fixed size এর packet গুলোকে Numbering করে যাতে packet duplicate না হয়, হারিয়ে না যায় অথবা মিসিং না থাকে।

2] Data Routing:- Most efficient path.

3] Data Formatting:- Rules for which group of bits or characters within packet constitute data or other information.

4] Flow Control:- Control a fast sender where the receiver is slow. It protects data transmission from traffic Congestion.

5] Error Control:- Detecting error messages then discarded by receiver & resend by sender.

6] Precedence & Order of transmission:-
Rules that ensures chance to use the Communication lines & other resources of the network based on priority.

1] Connection, Establishment & termination:

How connections are established, maintained & terminated.

2] Data security:- It prevent unauthorized access.

3] Log info.:- Software that consists of all jobs & communication tasks that have taken place.

By using this information users are charged.

Ext-22 (45)

Elements of a protocol

Syntax:- Structure or format of the data.

Semantics:- What action or decision to be taken based on the interpretation.

Timing:- → Tells receiver about readiness.
→ Tells sender about sending.

TCP (Transmission Control protocol):-

→ Responsible for dividing messages into packets.

→ It also ensures the destination of message data & all the info of msg datas.

IP (Internet protocol):-

What if the present you sent to your friends is received by your father? So, IP is responsible for handling the addresses.

Type of Data Communication

Simplex Com.:- One device only sends data & another only receives. Ex: IOT, data in keyboard

Half-Duplex:- Both can send & receive but not at the same time. Ex:- Walkie-Talkie.

Full-Duplex Com:- Two way com. Both can be done Ex:- Mobile phone.

Transmission Media or Com. Channels

(1) Guided Media:- Also called as wired media. Twisted pair, Coaxial cable → Electric signals Optical cable → Light signals.

Twisted pair (i) Unshielded: used widely, Does not protects from external interface, cheaper Shielded.

(ii) Shielded:- Have extra interface used to protect. Heavier & costlier than UTP.

Coaxial Cable:- Consists of a solid wire core that is surrounded by one or more foil or wire shields.

Inner core carries coaxial cable

Outer shield provides the ground

Better but expensive than twisted pair.

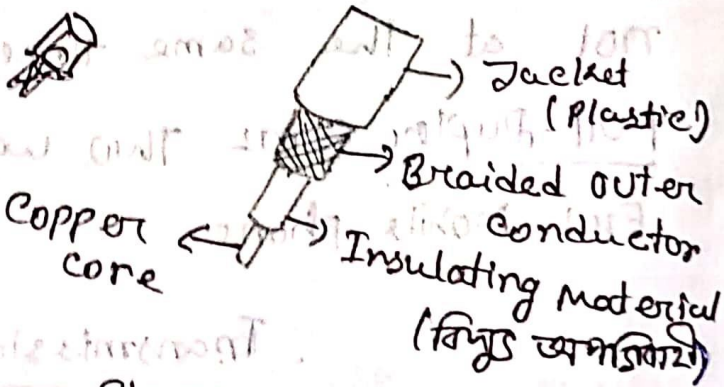


Fig:- Coaxial Cable.

Optical Fibers:-

Transmits large amount of data at very high speeds due to which it is widely used in Internet cables. It carries data as a light that travels inside a thin glass fiber.

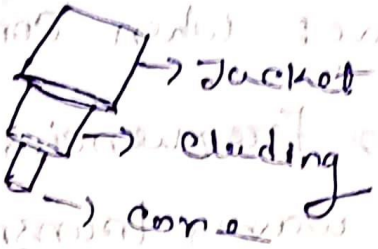
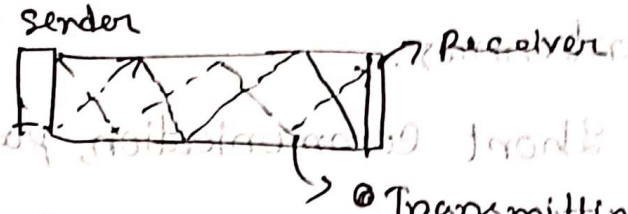


Fig:- Optical Fiber



* Transmitting signal in light sped.

Fig:- Data Travel through optical fiber.

Unguided Media

=> Signals are propagated from one device to another wirelessly. And signals can wave through wave, air, vaccum etc. Also divided in many parts :-

1] **Microwave:-** It offers communication without the use of cables. Used in long distance com. It is consisted of transmitter, receiver & atmosphere. And there is a parabolic antenna which is placed on the towers. The ~~greater~~ higher the tower is, greater the range.

2] Radio wave:- When com. is carried out by radio frequencies, then it is termed as radio waves transmission. Offers mobility. Consists of transmitter & the receiver both use antennas.

3] Infrared:- Short communication, passes through any objects. Ex:- TV, Remote, Wireless Mouse etc

Ethernet cable

→ Used for high speed wired network Connection between two devices. Four pair cable. Used for data transmission. at both ends of the cable, which is called RJ45 Connector.

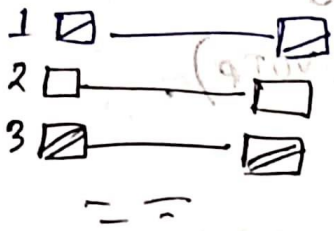
Ex:- Cat 5, Cat 5e, Cat 6, UTP cable.

10/100 MBPS

10/100/1000 Mbps.

Straight Through:-

Each end have RJ45 connectors. And each has the same pin out. Either T568A, T568B standards. To maintain consistency it has the same color type. It connects with ~~not~~ router. And most common type.



Crossover cable :-

One end is T568A & other end is T568B. Pin 1 is crossed with pin 3. And pin 2 is crossed with pin 6.

Widely connects for two devices at the same type. Ex:- Two computers or two switches to each other.

It looks similar two regular Ethernet cables but its wiring is different & complex. It is used to connect two hosts directly.

Diff Difference between crossover & StraightThrough cable.

[3] Why we need Computer Net?

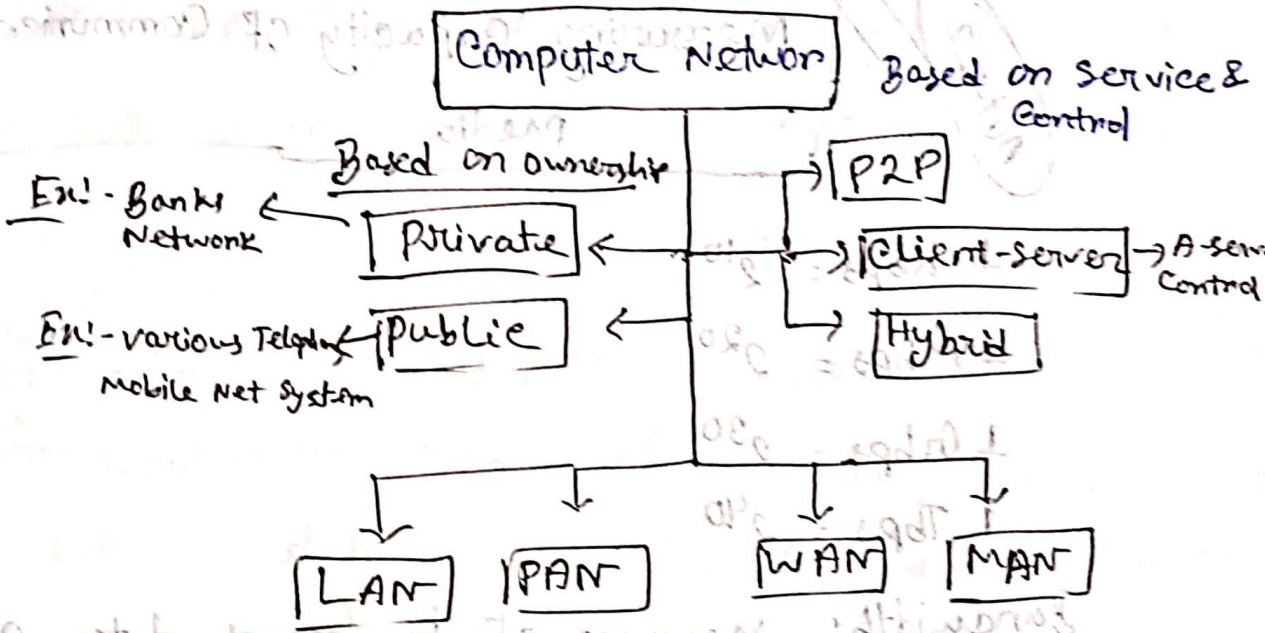
(1) File Sharing.
(2) Hardware Sharing
(3) Application Sharing.
(4) User Communication
(5) Network Gaming
(6) Voice over IP (VoIP).

[4] Architecture:-

Two types:-

(i) peer to peer (P2P). → Each Computer act as a both client & server.

Types of Computer Network:



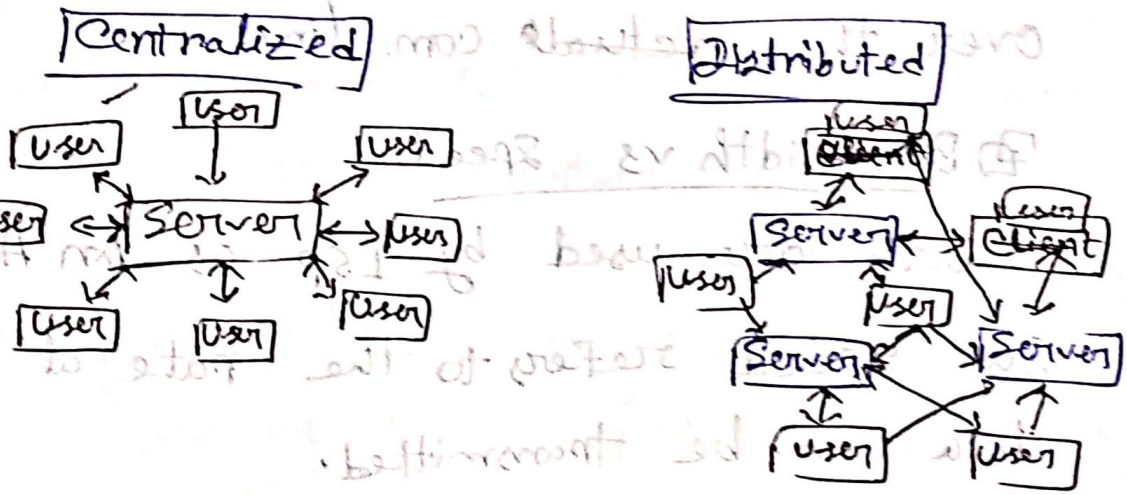
(Details in pdf - 32)

Prev

Client server: Server controls, give security.

(i) Centralized Server Network

(ii) Distributed Server Network.



Upto 5% is in HSE Note

AUT-22

Measuring Capacity Of Communication Media

1 Kbps = 2^{10}

1 Mbps = 2^{20}

1 Gbps = 2^{30}

1 Tbps = 2^{40}

Bandwidth:- Measure of how much data over time a communication link can handle its capacity.

Latency:- Time a packet goes from sender to receiver.

Throughput:- Data successfully sent/Received over the actual com. link.

Bandwidth vs Speed:-

=) Both are used by ISP as an Advertisement But Speed refers to the rate at which data can be transmitted.

And Bandwidth means the capacity of internet.

Bandwidth vs Latency:-

Latency is ping rate. The lag in network.

Bandwidth → info sent per second

Latency → info coming to the source

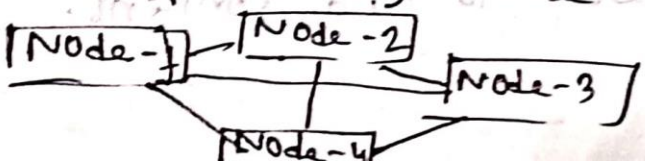
Bandwidth vs Throughput:-

Throughput → How much info actually gets delivered in a certain amount of time.
(How much of the data makes it to the destination).

Network Architecture:- peer to peer, Client-server

Aut-22

P2P:- Two or more pcs share files & access to devices such as printers without requiring a separate server computer or server software. Each node or workstation have same capabilities. Each peer is equal to other peers. NO center of the network. Most egaltarian ( ) network. Each peer has same responsibilities.



How P2P works?

Web browser website plays the important role in it. It plays the role of server & computer of user work as a client. This model performs their tasks like as one-way road while downloaded data moves from website to pc.

But in P2P connection it is handled in different way. If someone tries to download a file it uses some other pc as server where the file is already downloaded.

And scenario works as 2 ways road. All files are converted into bits of data which come from user's pcs but it is released after sending requests.

2 Types of P2P:-

(1) Unstructured :- Network is easy to build & devices are connected randomly. But it is hard to find content.

2) Structured :- Is designed using virtual layer in order to put the nodes in a specific structure Hard to set up.

Advantage :-

Disadvantage :-

Client - Server Network

Hosting websites (websites) → web Server

File Transfer protocol Servers → (FTPS)

Domain Name Service Server → DNS

(If someone browse to the a website name name study.com the DNS server will give specific routing info.

Dynamic Host Configuration protocol Server (DHCP)

↳ This includes how to access the local Network as well as how to exit the local Net to gain access of Internet.

Types of servers :-

(i) File servers :- Store, retrieve, moves data.

(ii) Printer Server :- Manage printing in the network.

(iii) Application Servers :- Expensive soft. & Additional computing

Power :- Can be shared by the computer.

Message server :- Interaction between users, documents, Applications. Data can be used in the form of audio, video, binary, text or graphics.

Database Server :- Type of Application Server

- Advantages :-
  - (i) centralized :-
  - (ii) security
  - (iii) Performance
  - (iv) Scalability
- Disadvantages :-
  - (i) Traffic Congestion

Networking Devices & Functions

(i) Repeaters - Regenerate signal before it gets weak. 2 port device

(ii) Hub :- multiport repeater

Ex :- Connector of star Topology.

Types: (i) Active Hub:- Have own power supply, can clean, boost & relay the signal along the network.

(2) passive Hub:- Collect wiring from Nodes & power supply from active Hub.

Bridge:- Repeater with add on functionality of Filtering content by MAC addresses. Has a single input & output port. 2 port device

Types:- (i) Transparent Bridges:-

(ii) Source Routing Bridges

Switch:- Multiport bridge with a buffer & a design that can boost its efficiency & performance. It does error checking it does not forward any erroneous data. Divides collision domain of hosts, but broadcast domain remain same.

Routers:- Routes data packets based on the IP addresses. Connects LAN & WAN together.

Divides broadcast domains of hosts connected through it.

Gateway:- Passage to connect two networks together that may work upon different Networking Models.

Router:- Combine Features of both bridge & Router.

Modem:- Modulator-Demodulator.

→ Converts Digital sig. to Analog signal

→ " Analog " to Digital "

2 types →(i) External

(ii) Internal.

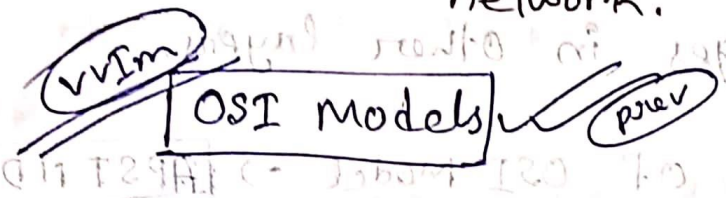
Access point (AP)

Internetworks:- Computer networks with other networks. The resulting system of interconnected networks is called internet.

Internet is collection of networks located all around the world that are connected by Gateways.

internet (lowercase 'i') → Generic term used to mean an interconnection of networks

Internet (uppercase 'I') → Mean Specific worldwide network.



Open System Interconnection (OSI) Model also defines a logical network & effectively describes Computer packet Transfer by using various layers of protocols.

Characteristics:

→ Layer should be created where the definite level of abstractions are needed.

→ Each layer should be selected as Internationally standardize protocols.

→ The number of layers should be large that seperate functions should not be put in the same layer. And architecture small enough so that it does not become complicated.

→ Each layer ~~perfo~~ relies on next layer to perform primitive functions. Every level should

be able to provide services to the next higher layer.
→ Changes in one layer should not need changes in other layers...

7 layers of OSI Model -> APSTNDP

(1) Applications

The upper layers (APS)

Application → presentation → Session

→ Mostly implemented in S/w.
→ Communication from one end user to another begins by using interaction b/w the App layer.

Heart of OSI (Transport)

The lower Layers (NDP):-

Network → Data Link → Physical

→ Handles activities related to Data Transport layers
→ Physical Layers
→ S/w & H/w

Physical layer:

→ Activate, Deactivate & maintain Physical Connection

→ Define voltages & Data rates needed for transmission.

→ Digital bits into electrical signal

→ Decide the transmission Full Duplex, Simplex or half-Duplex

Data Link Layer:

→ Connect errors that can correct error of physical layer.

→ Define protocol of two connected devices.

→ IP address which helps to identify any endpoint

→ Helps routing packets in the network.

→ Helps in defining best path which allow to data to flow from source to destination.

→ Data is subdivided into two layers.

(i) Media Access Control (MAC) layer:

Responsible for controlling how device in a network gain access to medium & permits to transmit data.

(ii) Logical link control layer: Allows to find error

(iii) Transport layer

- provide data transform from source to destination (divides the message into segments).
- Routed using single or multiple networks.
- Maintains quality of service functions.
- How, where, what data will be sent
- Rules of data.
- Layer build on the message that are received from the application layer.
- Helps ensure that data units are delivered error free.
- Offers acknowledgement of the successful data transmission sends the next data if no errors occurred.
- Example: TCP

Network Layer

→ Route signals through various channels to the other end.
→ Act as network controller
→ Divide outgoing messages
→ Assembles incoming packets.

Session Layer

→ Establishes, maintains & ends a session.
→ Enables two systems to enter into a dialog.
→ Allows a process to add checkpoints to stream of data.

Presentation Layer

Also known as Syntax layer. Data compression & Encryption.

Works!.

→ Character code translation from ASCII to EBCDIC.
→ Allows to reduce the number of bits that needs to be transmitted on the network.
→ Encrypt Data.
→ Provide user interface

Application Layer

→ Helps in identifying partners.
→ Determining resource availability.
→ Synchronizing com.
→ ~~Log~~ users to log on remote host.
→ provides various e-mail services.
→ Offers distributed & database sources.

Advantage

Disadvantage:-

~~Disadv~~

Aut-22

Lecture - 6

TCP/IP Model & DHCP

→ Helps to determine how a specific computer should be connected to the internet & how data should be transmitted between them.

⇒ TCP/IP (Transmission control protocol/ Internet protocol) stack is specifically designed as a model to offer highly reliable & end-to-end byte steam over an unreliable internetwork. It has different layers. Where each layer has different task to perform.

1] Application Layer (To allow access to Network sources.)

2] Transport [To provide process to process message delivery & error delivery]

3] Internet [To move packets from source to destination.
-> To provide internetworking]

4] Network Interface [Responsible for the transmission for the between two device on the same network]

TCP/IP Layers	TCP/IP protocols
Application Layer	HTTP, FTP, Telnet, SMTP, DNS
Transport Layer	TCP, UDP
Network Layer	IP, ARP, ICMP, IGMP
Network Interface Layer	Ethernet, Token Ring, Other link layer protocols

HTTP:- Hyper Text Transfer protocol. This protocol allows us to access over the world wide web It transfers data, audio, video, text etc. It is known as Hypertext T.P. as it It has the efficiency to use in a Hypertext environment

SNMP:- Simple Network Management protocol. Framework used for managing the devices on the internet by TCP/IP protocol suite.

FTP: File Transfer protocol. Standard for the exchange of program & data file ~~access~~ across a network.

SMTP:- Simple Mail Transfer protocol. Supports mail. Used to transfer data in other mail address.

Telnet:- provide virtual terminals of remote systems on LAN.

DNS:- Domain Name System. IP address is used to identify the connection of a host to the internet uniquely. But people prefer to use names. And the system that maps the name to the address is known as DNS.

~~Transfer protocol~~

Transport Layer in TCP/IP model can be represented by three protocols:-

→ Transmission Control protocol (TCP),
→ User Data gram protocol (UDP),
→ Stream Control Transmission protocol (SCTP).

⇒ User Data gram protocol:-

→ P to P protocol

→ Takes data from upper layer of TCP/IP Model & adds following info to data:-

(i) Port Address

(ii) Checksum error control

(iii) Length of data.

Transmission Control protocol (TCP)

→ Connection oriented protocol

→ A connection between sender & receiver.

→ Creates small units called segments. Each segment is numbered so that it don't get lose at the receiver end.

→ It also has acknowledgement number if the data actually reached the destination or not.

Stream Control Transmission protocol:-

→ This protocol combines the best features of TCP & UDP.

→ Is used for voice data over internet.

Networking Protocol

Internetworking protocol (IP):-

→ Unreliable connectionless
→ Used for data transmission.
→ Does its best to send data but does not give guarantee.
→ Small packets known as datagrams. And these are transferred separately. But, they can take different route & duplicate data can be sent.

Internetworking:-

Arp:- Address Resolution protocol.
→ Discover the link layer Address.
→ Each device known as Physical Address usually imprinted on NIC

Reverse Address Resolution protocol (RARP):-

→ Helps to find the Internet Access address of a device whose physical address is known.

Internet control Message protocol (ICMP):-

→ ICMP sends datagram problems back to sender.

Internet Group Message protocol (IGMP):-

→ Used For simultaneous transmission of a message to a group of receipients

Three-Layer Hierarchical Model in Cisco

The first layer is the Local Area Network (LAN) that uses IEEE 802.3 Ethernet technology, provide security against unauthorized access. The next layer is WAN.

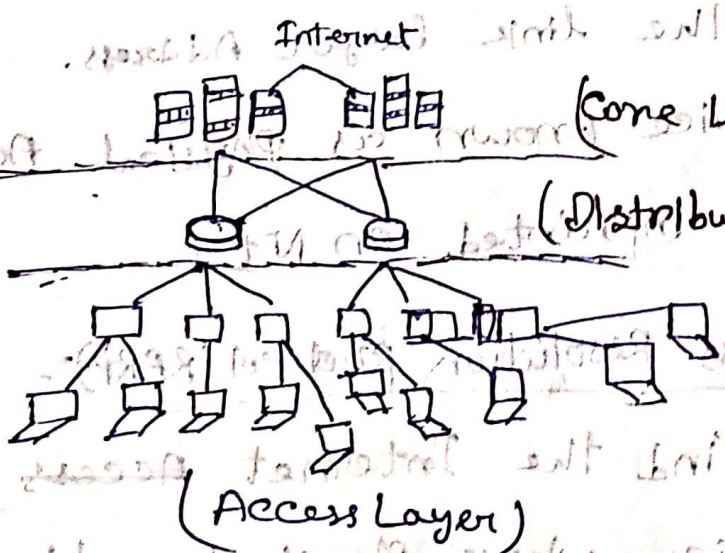


Fig 1- Three-Layer Hierarchical Model.

Three layers are:-

(i) The Access Layer
(ii) The Distribution Layer
(iii) The Core layer.

The Core Layers

It reduces Data latency, At ensuries data transfer in a faster way.

High to data Transfer Rate:-

→ Data speed is important
→ Through load sharing (Traffic can travel through multiple network connections) the speed can be increased.

Low latency period:-

→ Uses High-speed Low Latency circuits

High Reliability:-

→ Multiple path
→ If one path having problem then data can be sent through the alternative.

Equipments of Core layers:

→ Cisco switches: 7000, 7200, 7500 & 12000 (For WAN)
→ Catalyst " :- 6000, 5000, 4000 (For LAN)
→ T-1, E-1, SMDS, ATM Networks

Distribution Layer

Multiple Local Networks কে divide করে তাদের Distribution Layer (DL) ব্যবহারের মাধ্যমে করে। এবং Access layer থেকে Filter করে core layer এ দেয়। The router maintain a routing table to forward received data packet.

Packet filtering:

→ processes packets & regulate the transmission of packets based on its source & destination information to create network borders.

QoS: Layer 3 switches prioritize delivery based on policies

Access Layer Aggregation point:

→ serves point for the desktop layer switches.

Control broadcast & Multicast:-

⇒ Layer 3 serves as boundary for broadcast & multicast domain.

Application Gateways:-

→ Allows to create protocol gateways to & from different network Architecture.

→ একটা router দিয়ে অনেকগুলো Network create করা। বিভিন্ন user বিভিন্ন কিনিস browse করে। সব same gateway দিয়ে request যায়। তাই এই কারণে Application Gateway লাগে।

Access Layer

Devices that allow users to use the services provided by the distribution & core layers.

At access layer:-

→ Enable MAC address filtering : Allow only certain systems to access the connected LANs.

→ Create Separate Collision Domains :-

→ Switch can create separate collision domains.

Share bandwidth :- Same network connection to handle all dates.

Hand switch Bandwidth :- Move data from one to another.

Advantage of 3 layers

→ High Performance

→ Efficient Management & Troubleshooting.

→ Policy Creation.

→ Scalability.

→ Behavior prediction.

DHCP

Dynamic Host Configuration protocol. Is a network management protocol & it is allocated dynamically. DHCP automatically assign IP, subnet masks, Default gateway & DNS.

Component of DHCP:-

1] DHCP Server.

2] DHCP client :- gets info from server

3] DHCP Relay Agent :- Needs so that DHCP server can handle the request from all the networks

4] IP Address pool :- Lis of IP address

5] Subnet Mask :- In which network it is currently present

6] Lease Time :- Amount of time for which IP is available for client.

7] Gateway Address :-

AUT-2022-2(a)

How DHCP works?

Dynamically assign of IP address happens after DHCP transactions or DHCP Conversation.

DHCP Discovery:- DHCP client send a broadcast message to discover DHCP servers. And the packet is sent with a default broadcast destination of 255.255.255.255. It is a special address means "This network".

DHCP Offer:- After receiving packet from the Discovery server offers:-

IP address : (here 192.168.1.11)

Subnet : (here 255.255.255.0)

Default gateway:- (192.168.1.1)

DNS Server : (here 8.8.8.8)

DHCP request → (See last page)

DHCP Acknowledgement:- Sends acknowledgement to the client confirming the DHCP lease to the client.

Control of → See last page

Advantage:-

→ Easy to implemant
→ Automatic
→ Manual is not required
→ Saves time
→ Save workload
→ Duplicates are not there
→ Great benefit for mobile users.

Disadvantage:-

→ NO secure mechanism
→ Any new client can join the network.
→ Security risk for unauthorized access.
→ If server is one network might be failed

Point to Point protocol over Ethernet (PPPOE)

→ Commonly used in DSL
→ Isp telephone companies also use this.
→ There profiles are opened per person & It is used to track the user.

→ So that the connections are terminated under their control.

Data Transmission Method

used to establish link.

2 types :-

(1) Parallel D.T

(2) Serial D.T.

Parallel D.T

→ Multiple datas are sent at the same time over multiple channel.

Each channel carries one bit at the same time.

Is used :-

→ A large amount of data

→ Time sensitive

→ & Quickly.

Ex :- Video streaming.

Advantage:-

- → Easy to program
- → Faster.

Disadvantage:-

- → Requires more transmission channel.

[2] Serial Data Transmission:-

Block by Block or bit by bit Long data transmit এ use হয়।

Ex:- Modem, Mouse etc.

2 types: - **Advantage:-**

- → Only one T. Channel.

Disadvantage:-

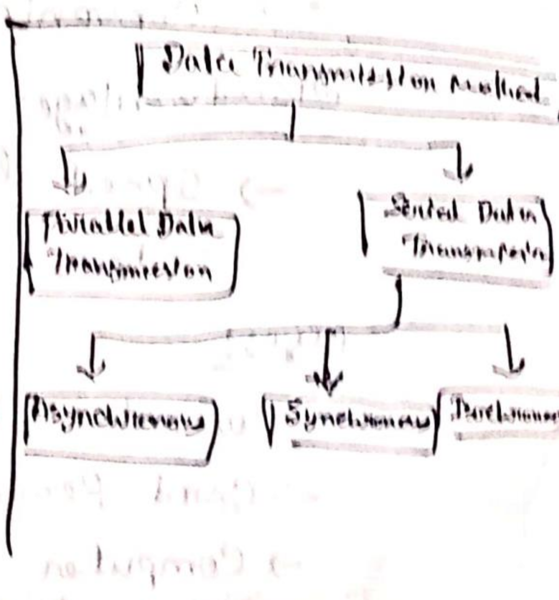
- → Slower data rate.

3 Types:-

[1] Asynchronous Transmission

[2] Synchronous "

[3] Isochronous "



Asynchronous Transmission:-

→ One character or one byte of data is sent from one device to another with uneven time time interval.

→ Stat bit in right sight so that receiver understand it.

Advantage:-

→ No synchronization

→ Sender does not need any primary storage device

→ Cost low.

→ Convenient for little amount of data

Disadvantage:-

→ Speed low

→ less effective.

Uses:-

→ Computer to Printer

→ Card Reader to Computer

→ Computer to Card Reader

→ Keyboard to Computer

Efficiency of Asynchronous

$$\text{Efficiency} = \frac{\text{Actual data bits}}{\text{Total bits}} \times 100\%$$

Here,

→ Actual data bits refers to the number of data bits to be sent.

→ Total bits refers to the sum of actual data bits & overhead data bits.

→ Overhead data bits are start bit (1 bit), stop bit (1 bit) & parity bit (1 bit)

Determine the efficiency of 20kB data transmission using Asynchronous Transmission Method.

⇒ Actual data = 20kB = 20×8kb
= 160kb = 160×1000 bit
= 160000 bit

Overhead data bit for each group = 3 bit
start, stop, parity = 3 bit

So, total overhead data needed for 160000 bit data = (3×8)×160000 = 60000 bit

∴ Total bits = Actual data bits + Overhead data bits

$= 160000 \text{ bit} + 60000 \text{ bit}$

$= 220000 \text{ bit}$

$\therefore \text{Efficiency} = \left(\frac{160000}{220000}\right) \times 100\%$

$= 73\%$

Synchronous Transmission

→ Transmits block by block. It has different sizes (128, 256, 512, 1024 characters)

Header info (16 bits) & trailer info (16 bits)

↓ beginning ↓ end

Advantage :-

→ Efficiency very high
→ Speed high
→ No need to transmit start & stop bit.
→ Method is suitable for a lot of datas.

Disadvantages:-

→ primary storage device is required.

→ Expensive

→ Synchronization between the source & target is required.

Uses:- Computer to Computer

Efficiency Math

(*) Determine the efficiency of 20KB data transmission using synchronous transmission method solution.

⇒ Actual data = 20KB = 20×8 Kb

= 160 Kb

= 160×1000 b

= 160000 b

Suppose, a block having 80 character = 80×8 bit

= 640 bit

Over head (Header & trailer info) bit = 16+16 bit

= 32 bit

∴ Total overhead data bits required

= (32/640) × 160000 bit = 8000 bit

∴ Total bits = (160000 + 8000) bit

= 168000 bit

∴ Efficiency = (160000 / 168000) × 100%

= 95%

Isochronous Transmission

Almost similar to synchronous transmission. But the time interval between blocks is almost zero.

In this transmission Synchronous & Asynchronous transmission data is collected from several devices within a time slot (125 ms) & then passed those collected data as time frame through a synchronous data link one after another.

Advantages:-

→ Speed much higher

→ No need to pause.

→ No start & end bit.

Disadvantage:-

→ primary storage device needed.

→ NOT possible if datas are received by the expected receiver or not.

→ NO error correction.

→ Expensive.

Uses:-

→ Real Time Application

→ In various multimedia com. like audio, video call

Bandwidth Calculation

File measure:-

1 KB = 1024 Bytes

1 MB = 1024 KB

1 GB = 1024 MB

1 TB = 1024 GB

Data Transfer Rate

1 Kbps = 1000 bits per second

1 Mbps = 1000 Kilo bits " second

1 Gbps = 1000 Mega bits per second.

*. Download Speed = ((Kbps x 1000) / 8) / 1024

20 Mbps का Speed क्या?

= 8. We know,

1 Mbps = 1000 Kbps

∴ 20 " = 20 × 1000 "

= 20000 Kbps

2. Speed = [(20 × 1000) × 1000 } / 8] / 1024

= 2441.41 KBps.

AUT-22

---. (শেষের অংশ)

[c] DHCP Request:-

→ Client receives DHCP offer message.

→ Client will Compare the offer that is requested

→ The client then send DHCP request. message.

→ Then the message is broadcast to the entire network.

⇒ Lease Control OF Lease Time:-

→ The client end the lease by sending a DHCP Release Message

→ Then server return the client's IP address to the available address pool & Cancel any remaining lease time.

Aut - 22

1(a) → P2P

1(b) → prev.

2(a) → prev

2(b) → prev

3(a) → Transport Layer (prev.)

~~3(b)~~ →

3(b)

Switching Concept required for:-

Switching concept is required for:- ~~too reqs~~

~~reason~~:-

Bandwidth:-

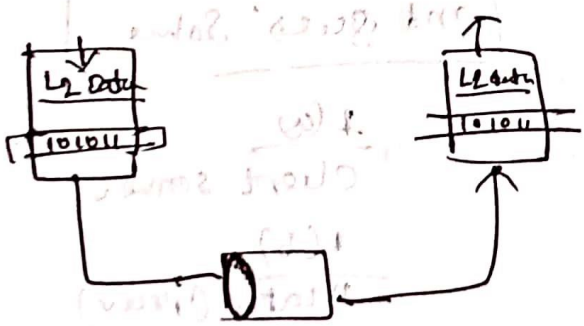
→ Said to be as the max transfer rate of a cable. very critical & expensive resource. Therefore, switching techniques are used for the effective utilization of the bandwidth of a network.

OSI Models

7 Layers:- APSTNDP

1. Physical Layer
2. Data-Link Layer
3. Network Layer.
4. Transport Layer.
5. Session Layer
6. presentation Layer
7. Application Layer.

Physical Layer



Transmission Medium

→ Lowest layer

→ Establish, maintain, Deactivates physical connection

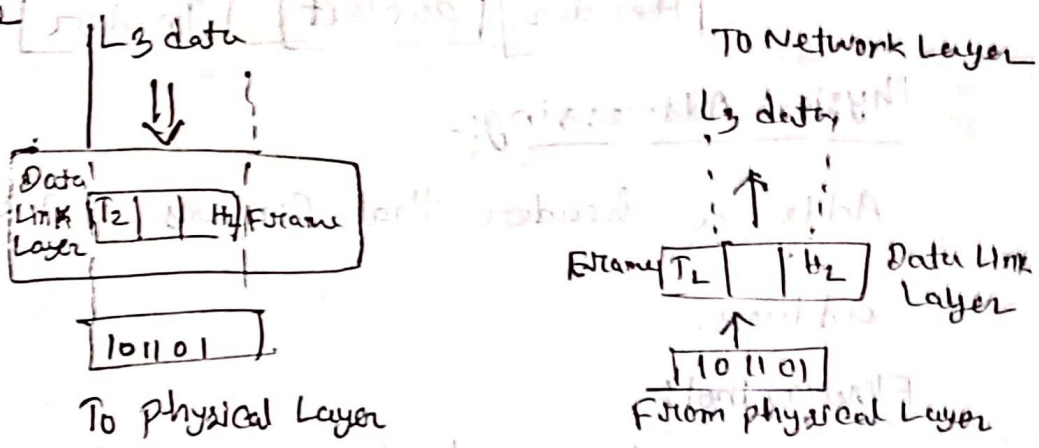
→ Mechanical, Electrical & procedural network interface specifications.

Functions of a physical Layer:-

→ Line Configuration
→ Data Transmission → (Simplex, Half-duplex, Full-duplex)
→ Topology.
→ Signals

Data Link Layer

→ ~~Unique~~

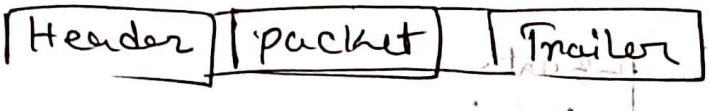


→ Unique Identification of each device.
→ Reliable & efficient communication between two or more devices.
→ Two sub-layers:-
(i) Logical Link Control layer:-
→ responsible for transferring the packets to the network layer.
(ii) Media Access Control Layer:-
→ Link between Logical & Network's Physical Layer.

Function:-

Framing:-

→ Data link layer translates the physical's raw bit stream into packets known as Frames. Header Contains Hardware destination & source address.



Physical Addressing:-

Adds a header that contains a destination address.

Flow control:-

→ Constant data rate is maintained. On both sides so that no data is corrupted.

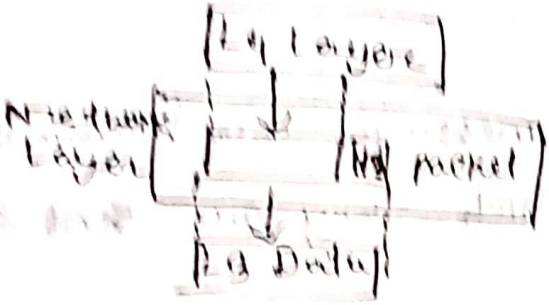
Error control :- Can be achieved by adding CRC (Cyclic Redundancy check).

Access control:-

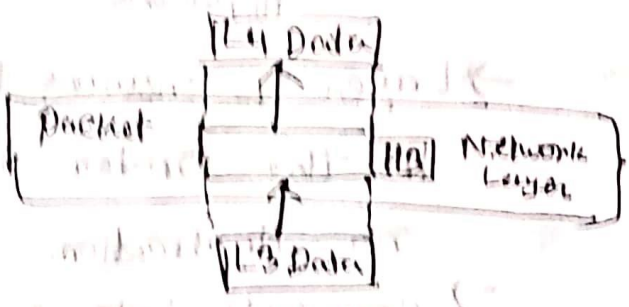
→ If two or more devices are connected to the same communication channel then the data link layer protocols are used to determine which device has control over the link.

Network Layer

- Manages device Packets location
- Determines the best paths.
- Routers are the Layer-3 devices.
- Protocols used to route the network traffic



To Data Link Layer

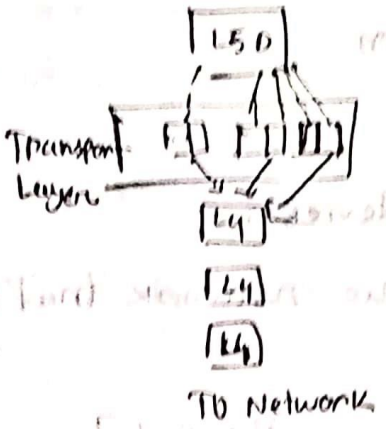


From Data Link Layer

Functions of Network Layer:

- Internetworking (Main responsibility of the Network Layer)
- Addressing (Source & destination are added to the Frame)
- Routing (Also Major Component of Network Layer)
- Packetizing (Receives packets & Converts them into packets).

Transport Layer

→ 

→ Layer-4 ensures that messages are transmitted in the order in which they are sent & no duplication.

→ Converts into smaller units

→ Two protocols:- → TCP (reorder packets at the receiver)
→ User Diagram protocol (Unreliable protocol. Cause sender keeps sending datas)

Functions:-

① Service-point Addressing:-

Transmit message to the correct process

② Segmentation & Reassembly:-

Transport layer receives from upper layer a message then it divides into segments & ~~sends~~ reassembles in the receiver ⊘ based on sequence numbers.

(3) Connection Control :- provides two layer services

(i) Connection oriented Service (All packet travel in single route)

(ii) Connectionless " (Treats each segment as individual Packets)

(4) Flow control :- perform end-to-end rather than single link.

(5) Error Control :- perform end-to-end. The sender transport layer ensures that message reach at the destination without any error.

Session Layer

→ Layer-3 OSI model

→ The Session layer is used to establish, maintain & synchronize the interaction between communication devices.

Function :-

(1) Dialog Control :- Creates a dialog between two processes

→ Allows Communication between two processes. Can be Half Duplex or Full Duplex

(2) Synchronization :- Adds some checkpoints when transmitting the data in a sequence. If error happen the transmission

will happen from the checkpoint.

Presentation Layer

→ Concerned with the syntax & semantics of the information.

→ Acts as data translator.

Functions:-

① Translation:-

→ Exchange the information in the form of characters strings, numbers & so on.

It converts data into common format & converts common format into actual data.

② Encryption:- Process of converting the sender-transmitted information.

③ Compression:- Reduce the number of bits.

Application Layer

→ Serves as windows for users.

→ Handles issues such as network transparency, resource allocation etc.

Function:-

① File transfer, access & management (FTAM):-

→ Allows user to access file in a remote computer.

→ To manage the files in a remote computer.

② Mail services:-

→ provides the facility for email forwarding & storage.

→ Provide distributed database sources & used to provide that global information about various objects.

Why do we still use the OSI Model?

In a networking stack, the OSI ~~con~~ architecture provides the principles needed to manage both technical problems & risks.

Despite the information security is changing to cloud-~~con~~ first environment, the OSI model

remains relevant:-

(1) Helps in identifying threats throughout our tech stack:-

=) As OSI is being used since the beginning so it is still relevant to use OSI.

Can assist in addressing vulnerabilities & security issues according to their layers they impact.

(2) Makes it possible to have a data-focused security posture:-

=) Determine where the security threads are. As it knows where the majority dates are kept (premises or in cloud).

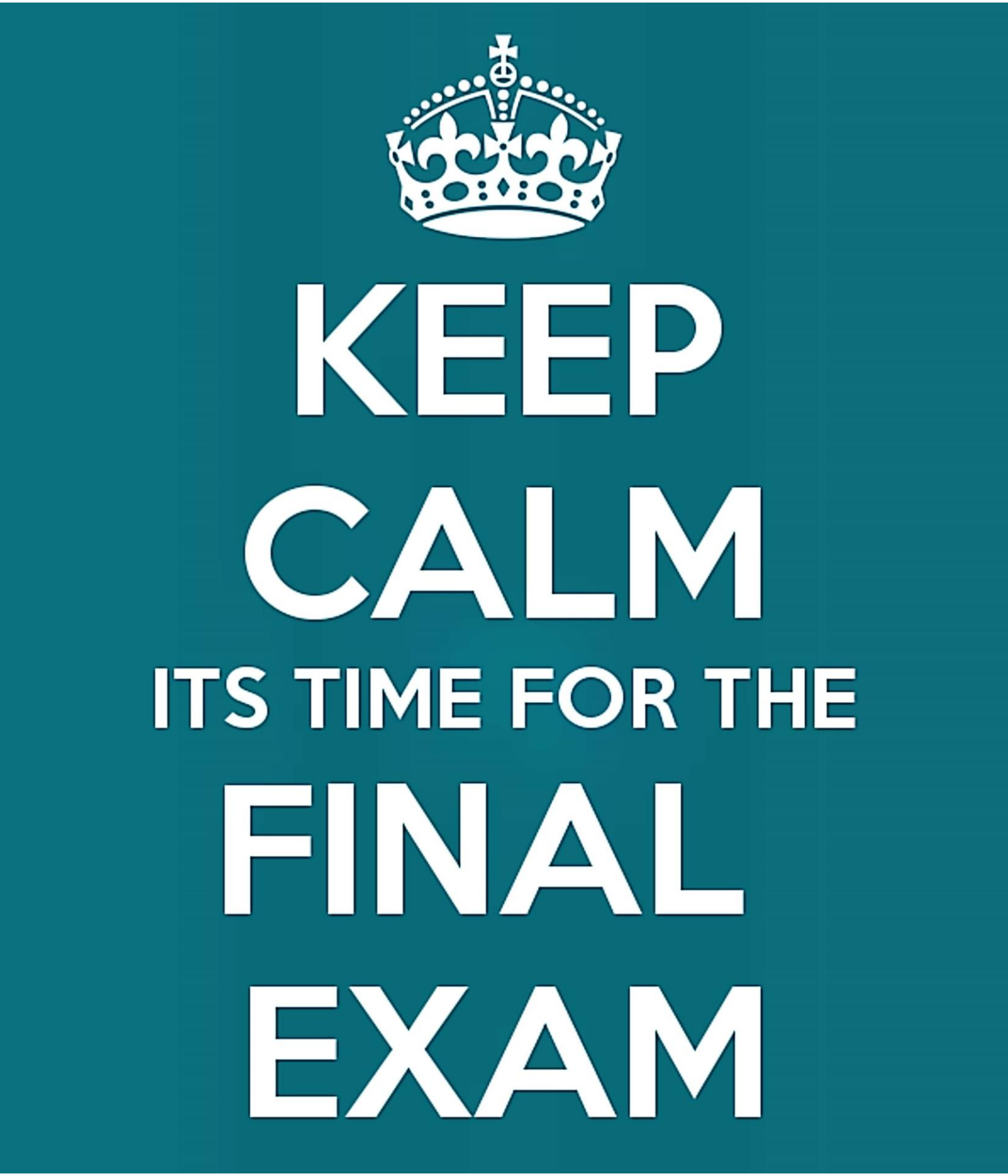
And this helps to keep the datas centralized knowing the datas are centralized gives extra security.

(3) Enables cloud adoption via a security First Approach

=) OSI model assist identifying the precise threads

(9) Secure cloud Infrastructure:-

⇒ Experts ~~updated~~ developed "updated" OSI models that reflect operational layers in Infrastructure as a service).


KEEP
CALM
ITS TIME FOR THE
FINAL
EXAM

FINAL

Multiplexing & Network Switching

→ Uses to combine & send the multiple data streams over a single medium. And the hardware is called as multiplexer.

→ Achieved by a device called Multiplexer (MUX) that combines n input lines to generate a single output line.

→ Demultiplexer (DEMUX) is used in receiver end. It separates each signal.

<u>Why Multiplexing :-</u>

→ Medium can have 1 signal at a time.

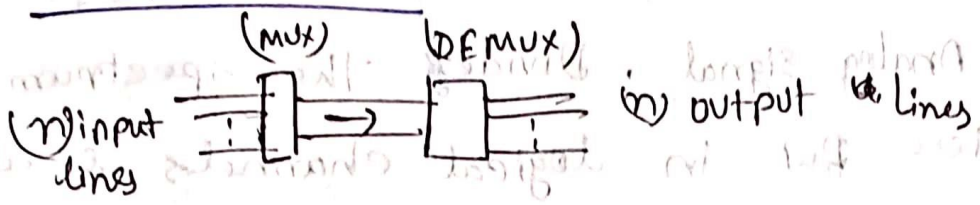
→ Multiple signal one medium share করলে তখন প্রতিটা ভাগকে divide করতে হবে যেন প্রতিটা signal-ই bandwidth পায়।

For Example :- 10 signals & BW of 100 units then 10 units is shared by each signal.

→ Multiple signal same medium share করলে Collision হতে পারে।

→ Transmission services are expensive.

Concept of MUX!-



→ Takes multiple signal

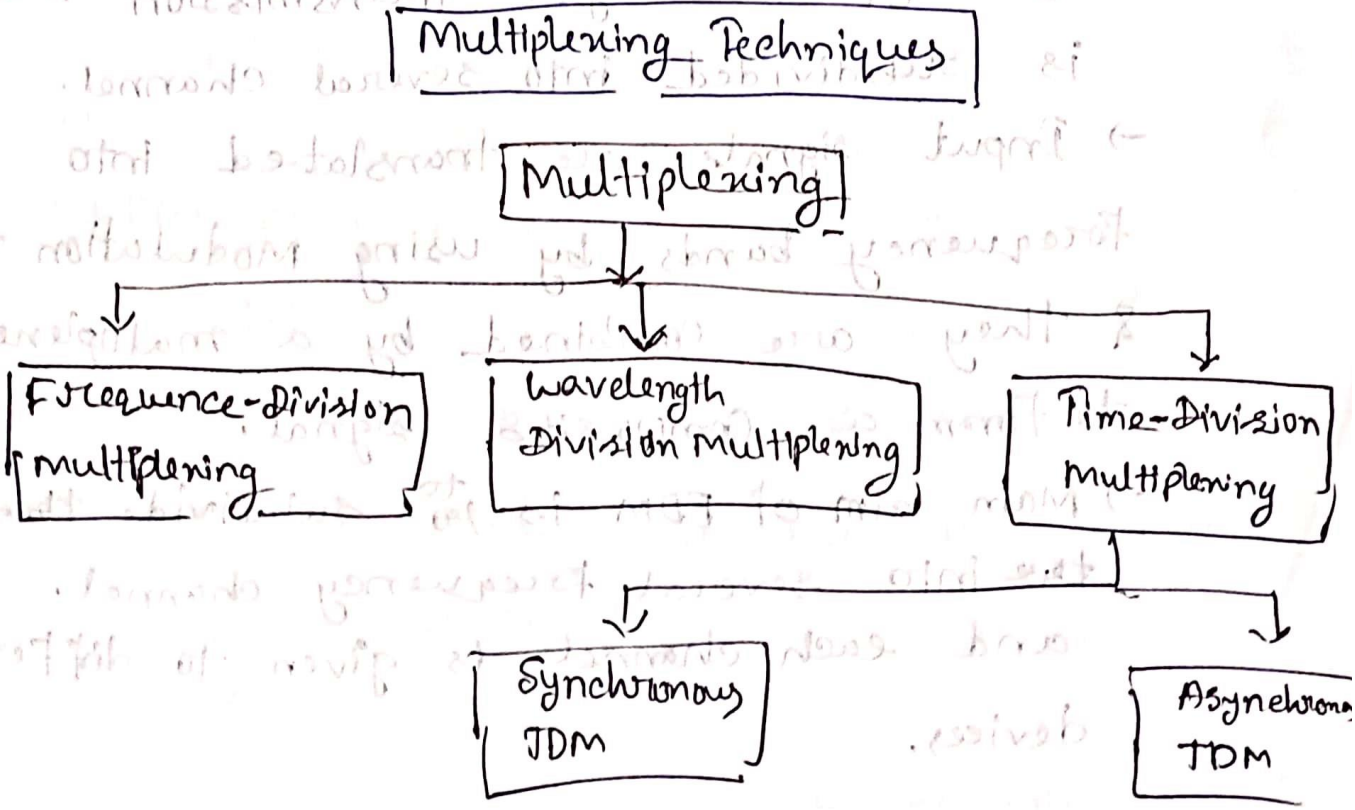
→ Creates one composite signal

→ Then gets separated by DEMUX.

Advantage!-

→ More than one signal can be sent

→ BW can be utilized effectively.



Frequency-Division Multiplexing (FDM)

FDM → Analog signal. Divides the spectrum or Carrier BW in logical channels & allocates one user to each channel. The are assigned in such a way so that they don't get overlapped.

Channels are separated by guard bands, which is not used by any channel.

→ It is an analog technique.

→ FDM is a technique in which the available BW of a single transmission medium is subdivided into several channel.

→ Input signals are translated into frequency bands by using Modulation techniques & they are combined by a multiplexer to form a Composite signal.

→ Main aim of FDM is to subdivide the into several frequency channel. and each channel is given to different devices.

→ Input signals are translated into freq band by using modulation techniques. And they are combined by a multiplexer to form a composite signal.

→ Main aim is to subdivide frequency & allocate them to form a composite signal. different devices.

→ Carriers that are used for modulation f1, f2, fn.

→ Mainly broadcasts TV network.

Advantages:

→ Used for Analog signals.

→ FDM process very simple & easy modulation.

→ Large number of signal can be sent.

→ Does not need synchronization between sender & receiver.

Disadvantage:

→ used only when low speed channels are required.

→ Suffers the problem of crosstalk.

→ A large number of modulators are required.

→ ~~Does not require any synchron~~

→ High BW needed.

Application:-

→ Commonly used in TV.

→ Used in FM & AM.

Wavelength Division Multiplexing (WDM)

→ Multiplexed into an optical fiber by using different wavelengths. An analog multiplexing technique & is done conceptually in the same manner as FDM but uses light as signals.

→ Total Amplitude of the wave.

How it is done?

⇒ WDM & FDM both are same but WDM uses optical signals.

→ WDM is used on fibre optics to increase the capacity of a single fibre.

→ An analog Multiplexing technique.

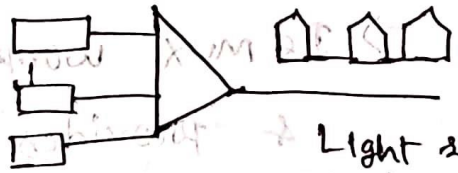
→ Optical signals from different source are combined together to form a wider band of light with the help of multiplexer.

→ To do this a prism are used.

→ In receiver ends demultiplexer separates the signals. And there prism is used too.

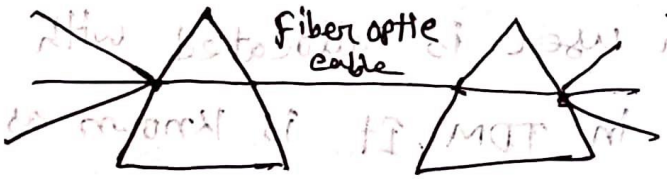
→ A prism can perform in a role to combine various optical signals to form a composite signal.

(a)



Light signal Transmission through optical Fiber

(b)



(c)

Fig. - WDM Transmitter

Time Division Multiplexing (TDM)

⇒ The shared channel is divided among its users by means of time slot. Each user can transmit data within the provided time slot only.

→ Works in TDM mode. MUX & Demux both are timely synchronized & both switch to next channel simultaneously.

Working:-

→ A transmits its frame

→ Demux provides media to channel A.

→ Time slot of A ends.

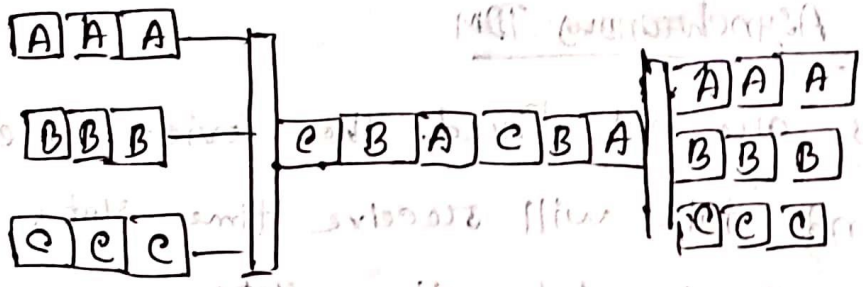
→ B time " starts.

→ Demux works in a synchronized manner & provides ~~chan~~ media to channel-B

→ Signal from different channel travels the path in interleaved manner.

Time slot:- Each user is allocated with different time interval in TDM. It is known as Time slot.

→ Can be used in both Analog & Digital But mainly used in digital.



→ TDM.

Synchronous TDM

→ Time slot is preassigned in every device

→ Device is given time slot even though there is no data.

→ If no data, then the slot will go empty.

→ Most popular synchronous TDM are T-1 mux.

ISDN & SONET MUX.

→ N device = N slots.

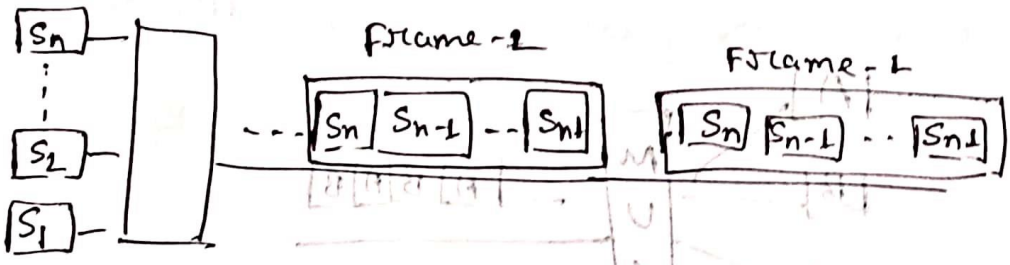


Figure :- Synchronous TDM

Disadvantages :-

→ Utilization is not good. As time slots can be ~~Empty~~. empty.

→ Speed of Transmission medium should be greater than the total speed of input lines.

Asynchronous TDM

→ Time slots are not fixed. The devices which need to send data will receive time slots.

→ Dynamically allocate ~~datas~~ time slots

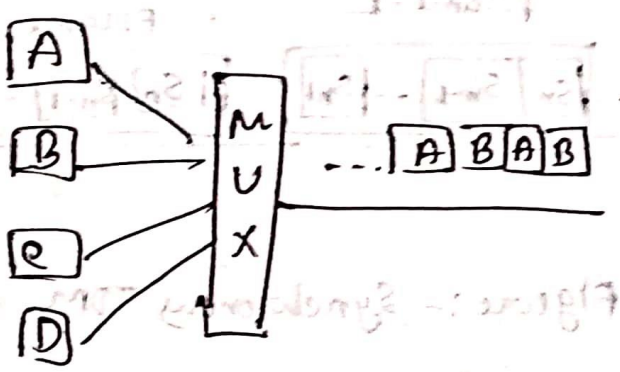
→ Total speed of input lines can be greater than the capacity of the channel.

→ Creates time slot only for those which are having data. NO empty time slot.

→ In ATDM there is an address part that identifies the source of the data.

→ It is fully utilized.

→ In ATDM if there are n sending data then there m time slots ~~(n<m)~~. (m<n).



Here 4 devices, but only two are transmitting datas.

Network Switching

→ Switch Data Transfer করে বা forward করে। আর এটা Mac Address দিয়ে নির্দিষ্ট device এ Data পাঠায়।

→ Transferring the information from one computer to network to another computer Network that is known as switching.

→ Switching is achieved by using switches. Switch is a small hardware device which is used to join multiple computers together with one local area Network (LAN). It is operated in Layer 2 (Data Link Layer) in OSI Model.

→ Switching is transparent & does not need to change any configuration in the home network.

→ Operated in full duplex mode packet collision is minimum. as it directly communicates from source to destination.

There are 2 categories:-

1] Connectionless:- path or NO previous handshaking is required & acknowledgement is optional.

2] Connection oriented:- path acknowledge करता है। Data circuit में forward करता है।

Switching concept required for 2 reasons:-

1] Bandwidth:- Max transfer rate of a cable.

2] Collision:- More than one device transmits the message over the same physical media. And to get rid of this switching technique is applied.

Advantage:-

→ Increases Bandwidth

→ Sends info to the correct destination.

→ Increases overall performance by reducing traffic.

→ Less frame collision.

Disadvantage:-

→ Expensive (switch)

→ Can't determine the network connectivity issue. → Proper design & configuration is required.

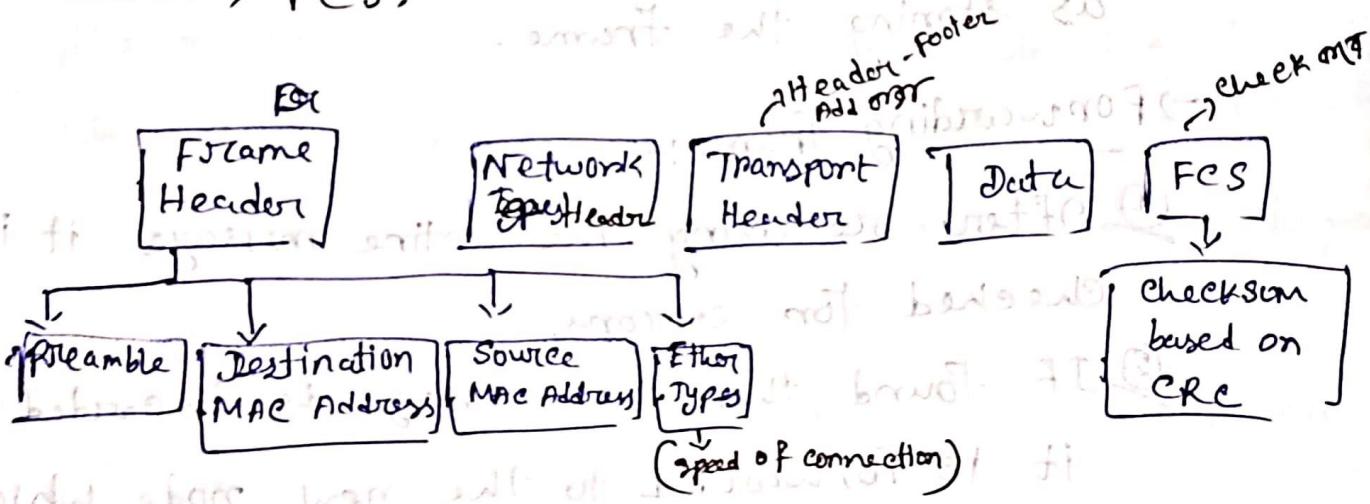
Switching Modes:-

→ Layer-2 switches are used for transmitting data on the data link layer,

→ perform error checking on received frames.

→ Mac Address ব্যবহার করে।

→ In switching Mode:- different parts of a frame are recognized. Frame consists of several parts such as. preamble, destination MAC Address, Source MAC Address, User's data, FCS.



3 types of Switching Modes:-

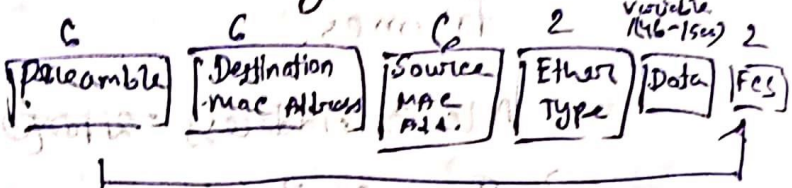
1] Store & Forward

2] Cut-Through

3] Fragment-free:

(1) Store-and-Forward :-

A technique where the intermediate nodes store the received frame & then check for errors before forwarding the packets to the next nodes.



→ Storing Frame:-

① Layer-2 switch waits until entire frame has received.

② After receiving this switch store the frame into the switch buffer memory. It is known as storing the frame.

→ Forwarding Frame:-

① After receiving the entire message it is checked for errors.

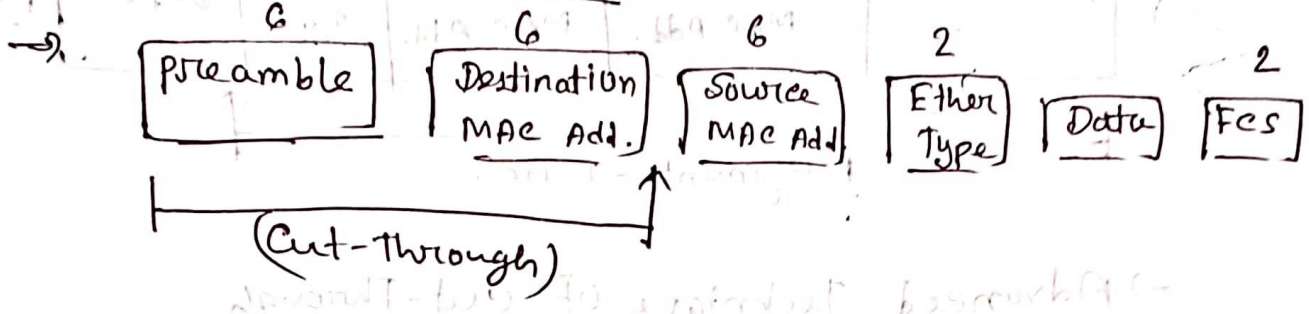
② If found then the message is discarded on it is forwarded to the next node. which is known as forwarding frame.

→ CRC (Cyclic Redundancy Check) is used for checking errors on the received frame.

→ This technique ensures a high level of security as the destination network won't be

affected by that. & also it does not collide.

(2) Cut-Through Switching :-



=) As soon as the destination address has been identified without waiting for the entire frame to be received.

→ After receiving, it checks first six bytes of the message following the preamble. The switch checks the destination in the switching table to determine the outgoing interface port & forward to the next destination.

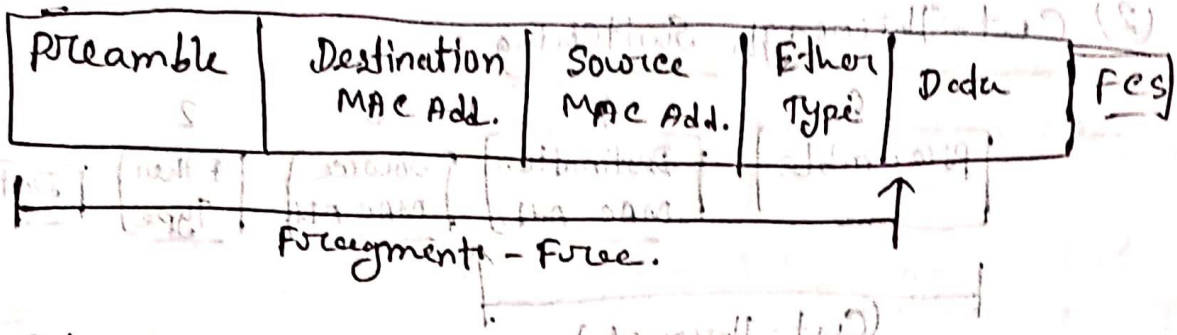
→ Low latency rate as the switch does not wait for the entire frame.

→ NO error checking technique.

→ Low wait time.

→ Collision can't be detected. If collided still it will be forwarded

(32) Fragment-Free Switching

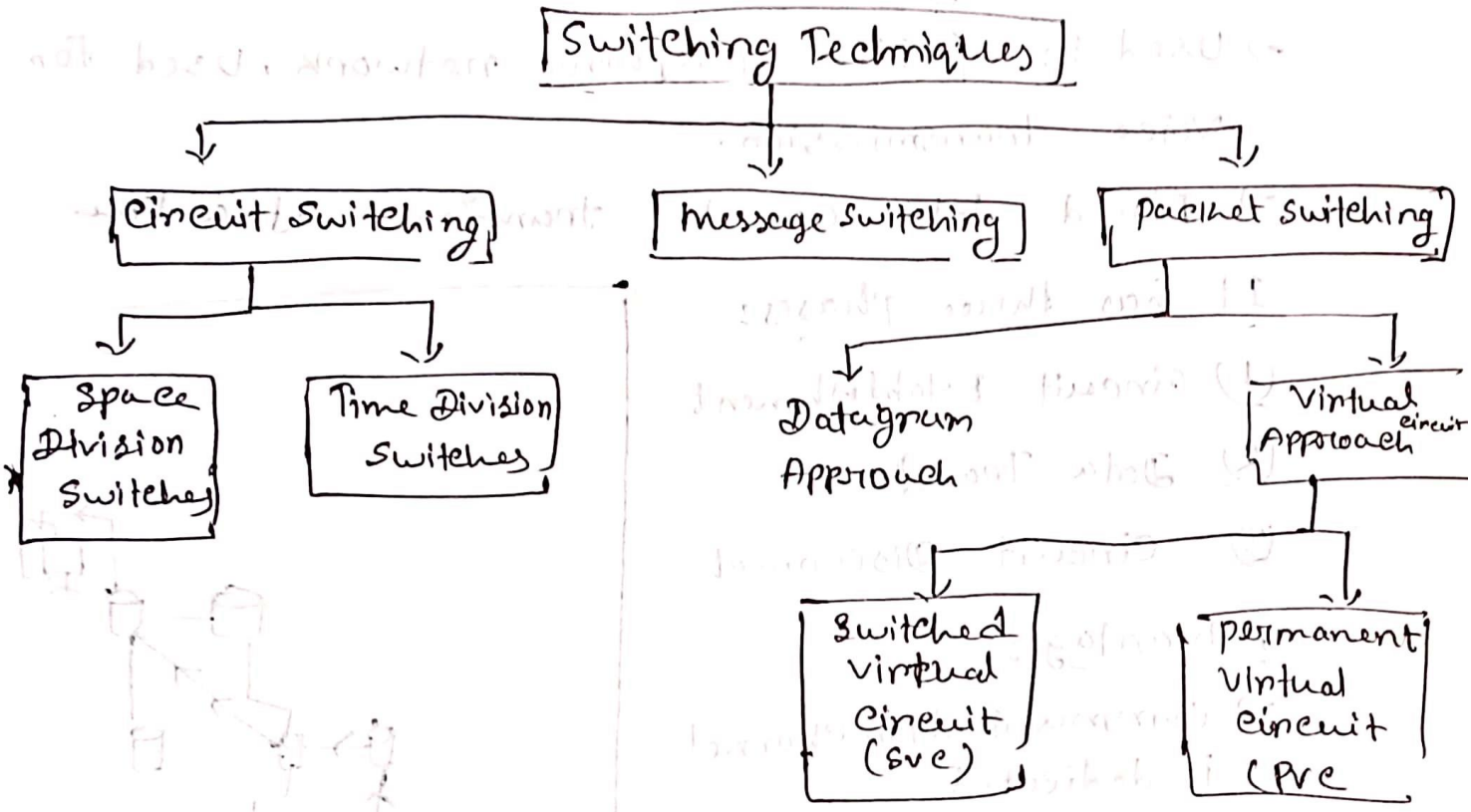


→ Advanced Technique of Cut-Through
→ Reads at ~~least~~ least 64 bytes of a Frame.
Error free transmission
→ Combines the speed of cut-through switching with the error checking functionality.
→ Checks 64 bytes of the ethernet frame where addressing info is available.
→ Collision is detected within 64 bytes of frame.

(Final 2D ...)

Switching Techniques

(Switching Techniques decide the best route from sender to receiver)



Circuit switching

(এখানে Dedicated path থাকে এবং CS)

- Dedicated path from sender to receiver
- Once connection is established it will be existing until it is terminated.
- Operates similar way as the telephone works.
- End to End path must be needed before the communication.

→ If sender sends datas (video, Audio) a request signal is sent to the receiver then the receiver sends back the acknowledgement. to ensure the availability of dedicated path.

→ Used in public telephone network. Used for voice transmission.

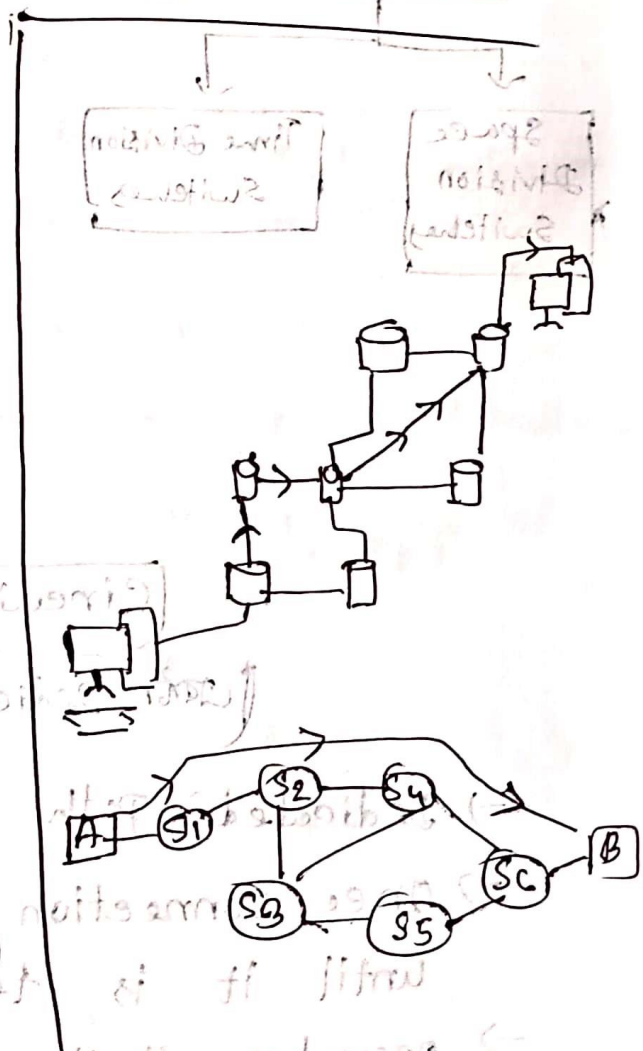
→ Fixed data can be transfered at a time

It has three phases:-

(1) Circuit Establishment

(2) Data Transfer

(3) Circuit Disconnect



Advantages:-

→ Communication channel is dedicated.

→ Fixed Bw.

Disadvantages:-

→ Only delay occurs in the sped of data transmission.

→ Takes long times to establish connection (10s Approximately)

→ More expensive

→ If no data is transferred then the capacity of the path is wasted.

→ No other data can be transferred if the channel is free.

Message Switching

(Data কোন path দিয়ে যাবে তা matter করে না। Source to Destination এ Message গেলেই হলো। per checkpoint এ Hop Count হবে। Based on Bandwidth এর path select করে।)

প্রথমে পুরো ম্যাসেজ Receive করে তারপর buffer করে যতক্ষণ না কোনো resource আছে পরবর্তী Hop এ যাওয়ার জন্য। আর যদি না হয়, তবে message store হয় এবং wait করে)

- → Transferred as a whole unit.
- → No dedicated path from source to destination.
- → MS provides Dynamic routing as the message is routed through the intermediate nodes.
- → Programmed in the way so that it can provide the most efficient routes.
- → Every node stores the entire message & then forward it to the next node.

Advantages:-

→ Data channels are shared among the communicating devices that improve the efficiency of using available BW.

→ Traffic congestion can be reduced.

→ Message priority can be used to manage the network

→ Supports the data of unlimited size.

Disadvantages:-

→ Must be stored until the message is forwarded.

→ Long delay can occur.

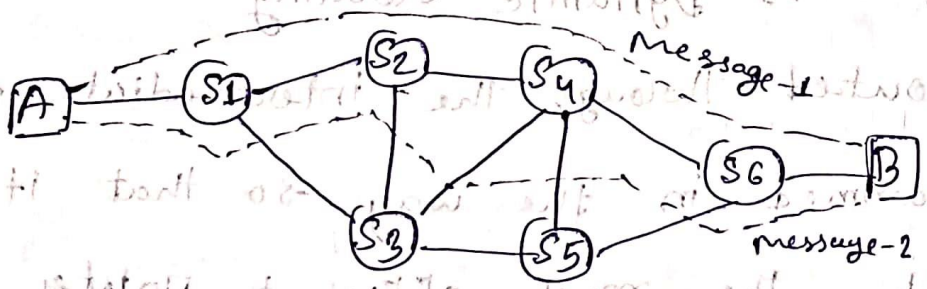


Fig:- Message switching

(Packet Switching)

(Packet আকারে send হবে। Different path দিয়ে যাবে। এতে efficiency বেশি।)

=> Easier for intermediate networking devices to store small size packets.

=> Divided into smaller pieces & they are sent individually.

-> They are given unique number to identify their order.

-> Every packets contains information, Header (Source Address), Destination Address & sequence number.

-> Packet will travel across the network. Take the shortest path as possible.

-> All packets will reassemble in the receiver.

-> If any packet is missing will be sent to resend it.

-> If all packets are received then message will be sent.

Fig:- Packet Switching

(VLSM) variable Length Subnet Mask

If your are assigned an IP Address 200.160.93.0/19 & asked to deploy VLSM. There are some requirements as follows:-

Ambarkhana = 800 hosts
Zindabazar → 90 hosts
Lamabazar → 1000 hosts
Subid Bazar → 150 hosts

Now assign network address for each area, also find broadcast address of those areas.

Ans:-

⊕ সবার host বেশি তার নিচে আগে কাজ শুরু হবে।

Here:- Given Address: 200.160.93.0/19

Subnet mask:- 11111111 11111111 11100000 00000000

Decimal:- 128 192 224 240 248 252 254

Block Size: ~~256 - 224 =~~ 32

Subnet:- 255.255.224.0

Block Size:- 256-224 = 32

200.160.0.0

200.160.32.0

200.160.64.0 /19

200.160.96.0

Lama Bazar (1000):-

$2^9 = 512$ | $2^{10} = 1024$ → Host Bit

Host bit = 10

Network bit = 32 - 10 = 22

Network Address:-

200.160.64.0/22

Subnet:-

11111111 11111111 11111100 00000000

255 . 255 . 252 . 0 → 6টা এর 252 (counting)

$\left(\frac{1024}{256} = 4 \text{ Block}\right)$

Broadcast Address:-

200.160.67.255/22

Amberkhana (800):-

$2^{10} = 1024$ (Host bit 10 টি নাহলে)

Host bit = 10

Network bit = 22

Network Address :- 200.160.68.0/22

Subnet Mask :- 255.255.252.0

Broadcast Address :- 1024/256 = 4 টি Block

200.160.71.255/22

IP loss :- 1024 - 800

= 224 টি

Subidbazar (150):- 28 = 256

Host bit = 8

Network bit = 32 - 8 = 24

Network Address :- 200.160.72.0/24

Subnet Mask :- 255.255.255.0

Broadcast Address :- 200.160.72.255

Zindabuzer (90):-

$2^6 = 64$, $2^7 = 128$

Host bit = 7

Network bit = 32-7 = 25

Network Address:- 200.160.73.0/25

Subnet Musk:- 255.255.255.128

Broadcast Address:- 200.160.73.255/25

VLSM From any given IP

Q 192.15.5.16/27 Find VLSM for this given IP.

A = 250

B = 60

C = 30

Binary Form of IP:-

192 . 15 . 5 . 16 /27 → 27 or bit Network, → HOST

11000000 . 00001111 . 00000101 . 000 10000

000 00000

192. 15. 5. 0 /24

A = $2^h - 2$

$= 2^8 - 2$

$= 254$

$32 - 5 = 24$

A= 192.15.5.0/24

255.255.255.0

192.15.5. 00000000

11111111

192.15.5. 255 → Broadcast Address

CIDR Math

/0 এরকম Subnet Mask → 0.0.0.0

কিন্তু এটা দিয়ে নেটওয়ার্ক কাজ করানো সমস্যাঃ। কারন 0.0.0.0।

আর Network এ Subnet Mask 255.0.0.0 হয় /8 এ হোলে। তাই এখান হতে use হয়।

FLSM

→ IP :- 192.168.1.0 /26

128 64 32 16 8 4 2 1 → octate

CIDR value মাথায়:-

/8 to /15 → Class A (0 to 15 Basically)

/16 to /23 → Class B

/24 to /30 → Class-C

/0 to /7 → Class A

Subne

/0 → 0.0.0

/3 → 128+64+32 = 224

/3 → 224.0.0.0

/8 => 128+64+32+16+8+4+2

=> 255

/8 => 255.0.0.0

128+64

192

(a) Subnet mask → 255.255.255.192 → /26 → 256 26

দুইটা open

So, 128+64 = 192

(b) Subnet network = /26 → 25.225 (2 টি)

$2^2 = 4$

(c) Host bit, 32-26=16

$2^h - 2 = 2^6 - 2 = 62$

(d) ③ valid Subnet = 256-192

= 64 → একেক Range হবে

→ Subnet Network বাড়ালে Subnet বাড়বে

(e) ⑤ Network Address

Table বানাতে হবে।

VLSM

256) 2046 (
× 7

→ Needed Size Column এর মোট

Assignable Range :-

256) 2046 (= 7.99 ≈ 8

192.168.0.1 - 192.168.7.254 - Broadcast

192.168.7.255

(c)

Host = $2^h - 2$

$= 2^{14} - 2$

$= 16384 - 2$

$= 16382$

(d)

valid Subnet = 256 - 192 = 64

(e)

	N-1	N-2	N-3	N-4
N.A	0	64	128	192
F.H.	1	65	129	193
L.H	62	126	190	254
Broad Add	63	127	191	255

N-1 :-

Network Address :- 172.15.10.0

F.H :- 172.15.10.01

L.H :- 172.15.10.62

B.A :- 172.15.10.63

N-2 :-

N.A :- 172.15.10.64

F.H :- 172.15.10.65

L.H :- 172.15.10.126

B.A :- 172.15.10.127

N-3

N.A :- 172.15.10.128

F.H :- 172.15.10.129

L.H : 172.15.10.190

B.A :- 172.15.10.191

N-4 :-

N.A :- 172.15.10.192

F.H :- 172.15.10.193

L.H :- 172.15.10.254

B.A :- 172.15.10.255

VLSM

Major Network :-

172.15.10.12/18

Subnet Name :	→	Needed Size :
A	→	1520
B	→	800
C	→	540
D	→	500
E	→	300

CIDR

CIDR	→	No. IP	→	Subnet
/32	→	1	→	255.255.255.255
/31	→	2	→	255.255.255.254
/30	→	4	→	255.255.255.252
/29	→	8	→	255.255.255.248
/28	→	16	→	255.255.255.240

CIDR	→	No. of IP	→	Subnet
/27	→	32	→	255.255.255.224
/26	→	64	→	255.255.255.192
/25	→	128	→	255.255.255.128
/24	→	256	→	255.255.255.0
/23	→	512	→	255.255.254.0
/22	→	1024	→	255.255.252.0
/21	→	2048	→	255.255.248.0
/20	→	4096	→	255.255.240.0
/19	→	8192	→	255.255.224.0
/18	→	16384	→	255.255.192.0

Subnet Name	Needed size	Allocated size	Address	Mask	Dec Mask	Assignable range	Broadcast
A	1520	2046	172.15.0.0	/21	255.255.248.0	172.15.0.1 to 172.15.7.254	~~172.15.10.8~~ 172.15.7.255
B	800	1022	~~172.15.10.0~~ 172.15.8.0	/22	255.255.252.0	172.15.8.1 to 172.15.11.254	172.15.11.255
C	540	1022	172.15.12.0	/22	255.255.252.0	172.15.12.1 to 172.15.15.254	172.15.15.255
D	500	510	172.15.16.0	/23	255.255.254.0	172.15.16.1 to 172.15.17.254	172.15.17.255
E	300	510	172.15.18.0	/23	255.255.254.0	172.15.18.1 to 172.15.19.254	172.15.19.255

Math:- VLSM!-

Major Network!- 172.15.10.12/18

Subnet Name:-	Needed Size
A →	1520
B →	800
C →	540
D →	500
E →	300

CIDR

CIDR	No. IP	Subnet Mask
/32	1	255.255.255.255
/31	2	255.255.255.254
/30	4	255.255.255.252
/29	8	255.255.255.248
/28	16	255.255.255.240
/27	32	255.255.255.224
/26	64	255.255.255.192
/25	128	255.255.255.128
/24	256	255.255.255.0
/23	512	255.255.254.0
/22	1024	255.255.252.0

CIDR	No. IP	Subnet mask
/21	2048	255.255.248.0
/20	4096	255.255.240.0

VLSM

Name of subnet	Needed size	Allocated size	Address	Mask	Dec Mask	Assignable range	Broadcast address
A	1520	2046	172.15.0.0	/21	255.255.248.0	172.15.0.1 to 172.15.7.254	172.15.7.255
B	800	1022	172.15.8.0	/22	255.255.252.0	172.15.8.1 to 172.15.11.254	172.15.11.255
C	540	1022	172.15.12.0	/22	255.255.252.0	172.15.12.1 to 172.15.15.254	172.15.15.255
D	500	510	172.15.16.0	/23	255.255.254.0	172.15.16.1 to 172.15.17.254	172.15.17.255
E	300	510	172.15.18.0	/23	255.255.254.0	172.15.18.1 to 172.15.19.254	172.15.19.255

FLSM

192.168.10.1/28

(a) Find the Subnet Mask Address:

(b) How many Subnets / Network?

(c) How many hosts per Subnet?

(d) Find the valid Subnet.

(e) Write the Network Address, Broadcast Address, 1st Host, Last Host address of each Subnet.

(a)

Here,

128 = (128+64+32+16) = 240

∴ Subnet Mask = 255.255.255.240

(b)

2^n =

Here, n = 4

$\therefore 2^4 = 16$

(c)

$2^h - 2 =$

Here, $n = 4$ & it is octate so, $h = 8-4 = 4$

$\therefore 2^4 - 2 = 16 - 2 = 14$

(d)

I have 240

$\therefore$ Valid Subnet $= 256 - 240$

$= 16$

(e)

	N-1	N-2	N-3	N-4
Net Address	0	16	32	48
First Host	1	17	33	49
Last Host	14	30	46	62
Broadcast	15	31	47	63

Network -1

Net Address :- 192.168.10.0

First Host : 192.168.10.1

Last Host :- 192.168.10.14

Broadcast :- 192.168.10.15

Q Find Ip address with any class following requirement of IT company.

(i) Four Remote Account dept with 250 user

(ii) Two remote HR → 100 user

(iii) Eight remote Agent → 600 user

(i)

Here Account Dept User = 250

∴ Host per Network = $\frac{250}{4} = 62.5 \approx 63$

140.20.10.1/26

Network = $2^n = 2^2 = 4$

Usable Host = $2^h - 2 = 2^6 - 2 = 62$

Valid Host = $2^h = 64$

Network Name	Network Address	Usable Host Address	Broadcast Address
A1	140.20.10.0	140.20.10.1 to 140.20.10.63	140.20.10.63
A2	140.20.10.64	140.20.10.65 to 140.20.10.126	140.20.10.127
A3	140.20.10.128	140.20.10.129 to 140.20.10.190	140.20.10.191
A4	140.20.10.192	140.20.10.193 to 140.20.10.254	140.20.10.255

(ii)

Host per Network $= \frac{100}{2} = 50$

$\therefore$ Network $= 2^1 = 2$

$\therefore$ Usable Host $= 2^7 - 2 = 126$

$\therefore$ Valid Host $= 2^7 = 128$

170.20.10.1/25

Net Name	Net Address	Usable Host Address	Broadcast Address
HR_1	170.20.10.0	170.20.10.1 to 170.20.10.126	170.20.10.127
HR_2	170.20.10.128	170.20.10.129 to 170.20.10.254	170.20.10.255

(iii)

$\therefore$ Host per Network $= \frac{600}{8} = 75$

$\therefore$ Network Needed $= 8 = 2^3$

IP: 180.30.10.1/19

Usable Host $= 2^h - 2 = 2^{13} - 2 = 8190$

Valid Host $= 2^{13} = 8192$

$\frac{8192}{256} = 32$

Net-Name	Net Address	Usable Host Address	Broadcast Address
Ag_1	180.30.10.0	180.30.10.1 to 180.30.31.254	180.30.31.255
Ag_2	180.30.32.0	180.30.32.1 to 180.30.63.254	180.30.63.255
Ag_3	180.30.64.0	180.30.64.1 to 180.30.95.254	180.30.95.255

Hope Count Math

Cost = 10^8 / Interface Bandwidth

Theory

IP Address

→ Required to communicate one computer with another.

→ To exchange information.

IP address

→ Private IP Address

→ Public IP Address

(1) Private IP address

→ Communicate within the same network.

→ Using private IP data or information can be sent within the same network.

→ Router supports this kind of IP

→ Private IP is assigned to all the devices which is inside the network three points

(2) Cons:- But private IP can be traced if this can be done using other devices in that network

Public IP address:-

→ Used to communicate outsider network.

⇒ 2 types:-

↳ Dynamic IP Address:- It changes over time.

After establishing connection of devices Isp provides this kind of IPs.

↳ Static IP Address:-

→ Don't change over time
→ permanent addresses.
→ Mostly used in DNS servers.

Public IP Addresses can be ~~changed~~ traced. back to the ISP which easily traced the geographical location.

But to rid from this using VPN is the best option.

Difference between private & public:-

private	public
1) Local	1) Global
2) Used to communicate within the network.	2) Outside the Network.
3) Connected to network in different ~~way~~ uniform manner.	(3) Non-Uniform manner.
(4) work on LAN	(4) Used to get Internet service.
(5) Used to load the Network operating system.	(5) Controlled by Isp.
(6) Available free of cost.	(6) ~~For~~ Not free of cost
(7) Can be known in ipConfig on Command Prompt	(7) public IP can be known by searching "what is my IP" on google
(8) 10.10.0.0 - 10.255.255.255	(8) Beside be private rest are public.
(9) Ex:- 192.168.1.10	(9) Ex:- 17.5.7.8
(10) Numeric code not unique Can be used again.	(10) Unique & Can't be used.
(11) Secure	(11) No security.

Private	Public
(12) Require NAT	(12) Require network Translation.

Subnet

→ Subnetwork within a Network

How to Create:-

3 main elements:-

(1) Network Address (Or) Subnet ID:- First Address of the subnet.

(2) Broadcast Address:- A packet forwarded to broadcast address is broadcasted to all.

(3) Subnet Mask:- Bit mask used to identify the subject of an IP address by applying bitwise AND operation with the netmask & IP Address.

(4) Point to point Subnet:-

→ point to point communication that directs communication between two routers. This subnet consist of a 31-bit subnet mask, leaving only two possible addresses in the network.

IPV6 Subnet:-

⇒ 128-bit length

⇒ 16 designated bits for subnetting act

→ 64-bits represents the network identifier

Benefits of subnetting:-

(i) Improved Network performance:-

→ Enables efficient communications between devices in a subnet & sends a packet for routing outside the subnet if a destination address isn't part of the subnet.

(ii) Enhanced Network Security:-

→ Reduce unauthorize access by isolating compromised subnetwork.

(iii) Simplified Network Management:-

IPv4 host addresses are classified into three classes:-

→ Class-A, B, C

Limitation of Subnetting:-

→ Requires router to communicate with each other (router)

→ wastes IP addresses.

→ Creating too many creates unnecessary complexity.

Data Network Security

→ Involves protecting the integrity, confidentiality, availability of data. It
It protects datas from unauthorized access.

Network Security vs Cyber Security

Network Security:-

(1) **Scope:-** protect's an organization's computer Networks, Systems & infrastructure. Involves safe guarding integrity, confidentiality & availability.

(2) **Components:-**

→ Components like Firewalls, detection, Access control, VPNs

→ Often involves H/w or S/w solutions.

(3) **goals:-** → Defend the network.

→ packet sniffing, port scanning, Network based attacks, DDoS, Malware.

(4) **Examples:-**

→ packet sniffing

→ Scanning

→ Standard devices like routers & Firewalls play a critical role in Network Security.

Cybersecurity:-

(i) Scope:- Broader protection of digital info, systems, devices & assets.

→ Includes network security & extends to securing applications, endpoints, data & org's digital ecosystem.

(ii) Components:-

→ Application security, Cloud, Mobile, Identity & Access Management, Threat intelligence & incident response

(iii) Goals:-

→ protect an org's digital assets from a comprehensive range of threats.

→ Safeguarding against cyberAttacks, Data breaches, Social Engineering, Insider Threats etc.

(iv) Ex:- Address issues like phising, ransomware, malware, Zero-day, data leaks. & compliance

[1] **Importance** -

(i) protection of sensitive data.

(ii) prevention of unauthorized Access.

(iii) Business continuity (Reduce & damage orgs reputation. Robust security measures may help)

(iv) Compliance & legal Obligations.

(v) Protection against malware

(vi) Prevents data theft & breaches

(vii) Preservation of reputation & customer trust

(viii) protection against Insider threats.

(ix) Global Connectivity.

(x) Security in the age of IOT

(xi) prevention of financial Loss

[2] **Works**:

(i) Physical Network Security (Relevent from physical access to routers, cabling etc. Locks, Biometric authentication etc helps)

(ii) Technical Network Security (Malicious activity from employees too)

(iii) Administrative Network Security (User using behavior & IT staff members work)

Network Security & Solutions:-

1) Firewalls:-
   (i) Hardware (Physical devices Filter)
   (ii) Software (Individual devices to serve & control)
2) VPN: Virtual private Networks (Encrypt data & provide secured access).
3) Encryption:-
   TLS & SSL protocol encrypt data transmitted over network.
4) Antivirus & Anti Malware S/W Device:- Trojan, Spyware
5) Security Information & Event Management (SIEM):-
   Collect & analyze log data from various network devices.
6) Network segmentation:- Divides a network into smaller segments.
7) Web-Application Firewalls:-
8) Email Security:- protects agains email-based attacks
9) Wireless Network Security:-
10) Security Patch Management:- (S/W & App Updates)
11) Content Filtering
12) Endpoint Security
13) Cloud security.
14) Security policies & Staff training.
15) Incidence Response & disaster Recovery

TCP/IP (Transmission Control protocol / Internet protocol) Security:-

(i) Encryption (Fundamental component of TCP/IP.

(ii) IPsec (Internet protocol Security):- protocol that secure IP communication.

(iii) Firewalls:- Critical component of TCP/IP. Control traffic flow.

(iv) IDPS:- Detects suspected activity.

(v) ACL:- Control network traffic by specifying rules.

(vi) Packet filtering.

(vii) Network Segmentation: Dividing into smaller

(viii) VLAN:- Separating networks.

(ix) Proxy Server

(x) DNS Security

(xi) Net monitoring & logging

(xii) Education & training.

DNS Security:-

(1) Domain Name System Security Extension

(2) DNS Cache poisoning (Hackers use to destroy data DNSSE helps in it)

(3) DDoS mitigation

(4) Anycast DNS (Helps distribute traffic & improves DNS service availability)

(5) DNS Filtering

(6) DNS Query Logging & Monitoring

(7) DNS Rate Limiting

(8) Security Training.

(9) Regular S/w updates
(10) Authoritative Server hardening

(B) (Web Security)

(1) Secure Socket Layer / Transport Layer Security
(2) Firewalls
(3) SQL Injection prevention (Malicious SQL code)
(4) Content Security policy.
(5) Two Factor Authentication
(6) Input validation (validating user data)
(7) Regular S/w Update
(8) Session Management
(10) DDoS Mitigation.
(11) Back up & Disaster recovery
(12) Training
(13) Access-control

(C) DNS Best practice:

(1) Audit the Network & security control:-
Helps overtime to understand what is going on.

(2) Using Network Address Translation:-
Gives internal protection to internal network. Enables fewer IP to confuse actors from learning which host they are learning.

(3) Use centralized logging & Immediate Log Analysis:

(4) Create Back up & recovery plan:-

(5) User Education

(6) Applying Zero Trust Philosophy.