Commputer Network & Communication

1. Requirements for Internet Connection

(i) Physical Connection → It is made by connecting a specialized expansion card such as modem or a network interface card (NIC) from a computer (PC) to a network.

(ii) Logical Connection → It uses standards called protocols. A protocol is a formal description of a set of rules & conventions that governs how devices on a network communicate. Connections to the internet may use multiple protocols.

(iii) Application that interprets data → The application that interprets the data & displays the information in an understandable form is the last part of the connection.

2. Network Interface Cards → The NIC communicates with the network through a serial connection & with the computer through a parallel connection. When selecting a NIC, consider the following factors:

(i) Protocols → Ethernet, Token Ring or FDDI

(ii) Types of media → Twisted-pair, coaxial, wireless or Fibre-optic

(iii) Types of system bus → PCI or ISA

3. TCP/IP Description & Configuration → TCP/IP is a set of protocols developed to allow computers to share resources. TCP/IP can be configured using the operating system tools.

• Network Topology is the schematic description of a network arrangement, connecting various nodes through line of connection.

CLASSTIME | Page No.
Date / /

4. Troubleshooting Internet Connections

(i) Define the problem (ii) Gather the facts
(iii) Consider the possibility (iv) Create an action plan
(v) Implement the plan (vi) Observe the results
(vii) Document the result (viii) Introduce problems & troubleshoot

5. Summary:-

(i) Computer recognizes & process data using a binary numbering system.
(ii) The number system used most frequently is the decimal number system.
(iii) The hexadecimal number system is used when working with computers because it can be used to represent binary numbers in a more readable form.

6. Data Networks

(i) Sneaker Network (ii) Local Area Network
(iii) Metropolitan Area Network (iv) Wide Area Network

7. Networking Devices

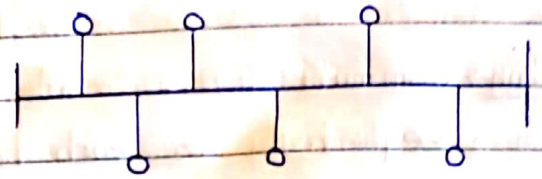
(i) End User Devices → PC, Printer, MAC, File Server, Laptop, IBM Mainframe
(ii) Network Devices → Repeater, Bridge, Small Hub, Workgroup 100 Base-T Hub, Router, Hub, Network Cloud

7. Network Topology → There are two types of topologies:-

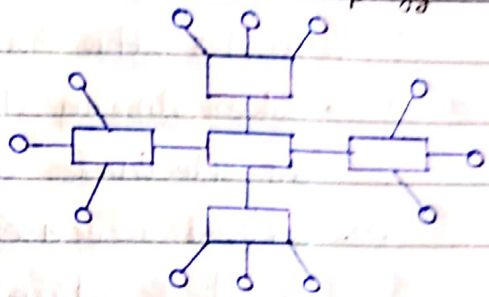
(i) Physical Topologies → It refers to the interconnected structure of of a local area network. The method employed to connect the physical devices on the

network with the cables & the type of cabling used all constitute the physical topology. There are six types of Physical topology :-

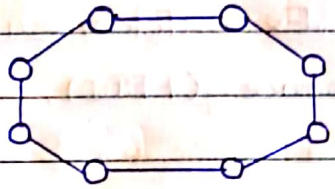
Bus Topology



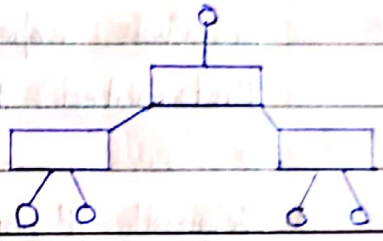
Extended Star Topology



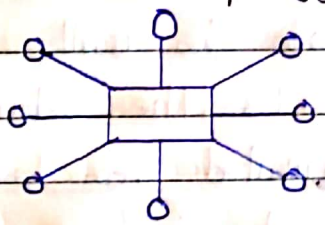
Ring Topology



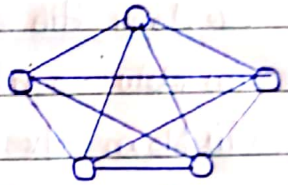
Hierarchical Topology



Star Topology



Mesh Topology



- Problem with Bus topology & Ring topology is that one system failure means whole topology failure.
- Advantage of star topology is that it fails only when central switch fails.
- Extended star topology is the base of all enterprise network. Only local area Network uses this.
- In Mesh topology, every node is connected to every other node.

iii) Logical Topologies → The logical topology of a network is how the hosts communicate across the medium. The two most common types of logical topologies are :-

Date / /

- Broadcast Topology → Each host sends its data to all other hosts on the network medium. There is no order that the stations must follow to use the network. It is First come, First serve. Ethernet works this way.
- Token Passing Topology → Communication is controlled by passing an electronic token sequentially to each host. When a host receives the token, that host can send data on the network. If the host has no data to send it passes the token to the next host & the process repeats itself. Ex:- Token ring, Fiber Distributed Data Interface (FDDI).

8. Network Protocols → Protocols controls all aspects of data communication, which include the following:
(i) How the physical network is built.
(ii) How computers connect to the network.
(iii) How the data is formatted for transmission
(iv) How that data is sent.
(v) How to deal with errors.

9. Local Area Network (LANs) → LANs are designed to:
(i) Operate within a limited geographical area.
(ii) Allow multi-access to high-bandwidth media.
(iii) Control the network privately under local administration
(iv) Provide full-time connectivity to local services.
(v) Connect Physically adjacent devices.
(vi) Using: Routers, Bridge, Hub, Ethernet switch, Repeater
(vii) Common LAN technologies are:- Ethernet, Token Ring, FDDI.

CLASSTIME | Page No.
Date / /

10. Wide Area Network (WANs) → WANs are designed to do the following:-

(i) Operate over a large geographically separated areas.

(ii) Allow users to have real-time communication capabilities with other users.

(iii) Provide full-time remote resources connected to local services.

(iv) Provide e-mail, World Wide Web, File transfer & e-commerce.

(v) Some common WAN technologies are:
- Integrated Service Digital Network (ISDN).
- Digital Subscriber line (DSL)
- Frame Relay
- US (T) & Europe (E) Carrier Series – T1, E1, T3, E3.
- Synchronous Optical Network (SONET)

(vi) Using: Routers, Communication Server, Modem CSU/DSU.

11. Storage-Area Network (SANS) → SAN technology allows high-speed server-to-storage, storage-to-storage, or server-to-server connectivity. SANs offer the following features

(i) Performance → SANs enable concurrent access of disk or tape arrays by two or more servers at high speeds, providing enhanced system performance.

(ii) Availability → SANs have disaster tolerance built in because data can be mirrored using a SAN upto to 10 Km or 6.2 miles away.

(iii) Scalability → Like a LAN/WAN, it can use a variety of technologies. This allows easy relocation of backup data, operations, file migration & data replication between systems.

CLASSTIME | Page No.
Date / /

12. Virtual Private Networks (VPNs) → A VPN is a private network that is constructed within a public network infrastructure such as the global market. Types of VPN:-

(i) Access VPN → Provide remote access to a mobile worker & small office / home office (SOHO) to the headquarters of the Internet or Extranet over a shared infrastructure.

(ii) Intranet VPN → Link regional & remote offices to the headquarters of the internal network over a shared infrastructure using dedicated connections.

(iii) Extranet VPN → Link business partners to the headquarters of the network over a shared infrastructure using dedicated connections.

13. Bandwidth → It is defined as the amount of information that can flow through a network connection in a given period of time.

(i) Bandwidth is finite
(ii) Bandwidth is not free
(iii) The demand for bandwidth is ever increasing.
(iv) Bandwidth is a key factor in analyzing network performance designing new networks & understanding the internet.

14. OSI Model → Benefits of OSI model :-

(i) Reduces complexity
(ii) Standardizes interfaces
(iii) Facilitates modular engineering
(iv) Ensures interoperable technology
(v) Accelerates evolution
(vi) Simplifies teaching & learning

CLASSTIME | Page No.
Date / /

14. OSI Layers → There are 7 layers present in OSI :-

Application
Presentation
Session
Transport
Network
Data Link
Physical

(i) Binary Transmission → Wires, connectors, voltage, data rates.

(ii) Data Link Control, Access to Media →
- Provides connectivity & path selection between two host.
- Provides Logical Address
- No error correction, best effort delivery

(iii) Network Address & Best Path Determination →
- Provides reliable transfer of data across media.
- Physical addressing, network topology, error notification, flow control.

(iv) Transport → End-to-end Connections :
- Concerned with transportation issues between hosts.
- Data transport reliability.
- Establish, maintain, terminate virtual circuits.
- Fault detection & recovery information flow control.

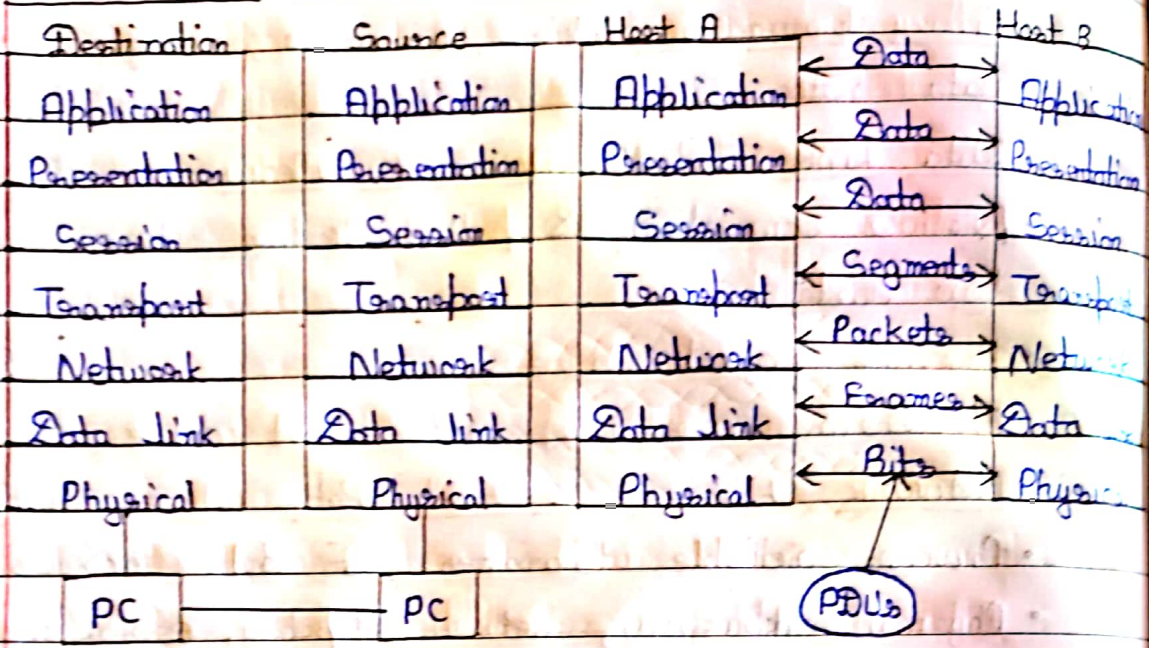
(v) Session → Interhost Communication
- Establishes, manages & terminates sessions between applications.

(vi) Presentation → Data Representation
- Ensure data is readable by receiving system.
- Format data
- Data Structures
- Negotiates data transfer syntax for application layer.

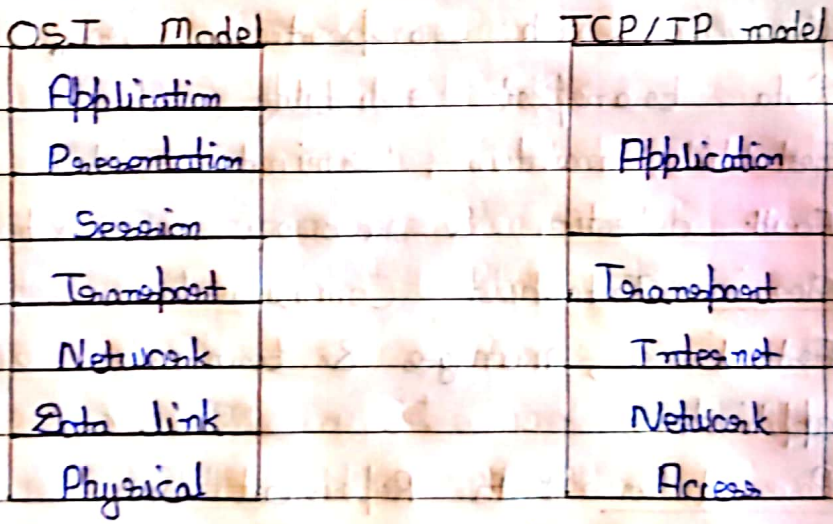
(vii) Application → Network Processes to Applications
- Provide network services to application processes (such as electronic mail, file transfer & terminal emulation).

CLASSTIME | Page No.
Date / /

15. Peer-to-Peer Communication



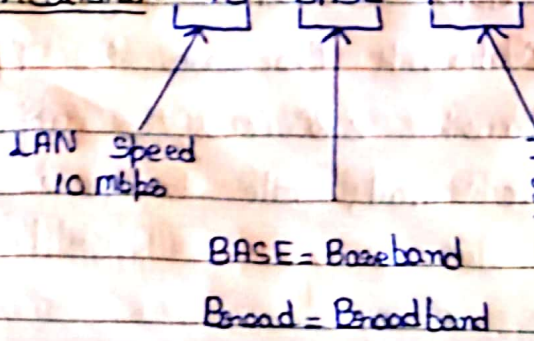
16. TCP / IP Model



TCP → Works mainly on Transport layer

IP → Works mainly on Internet layer

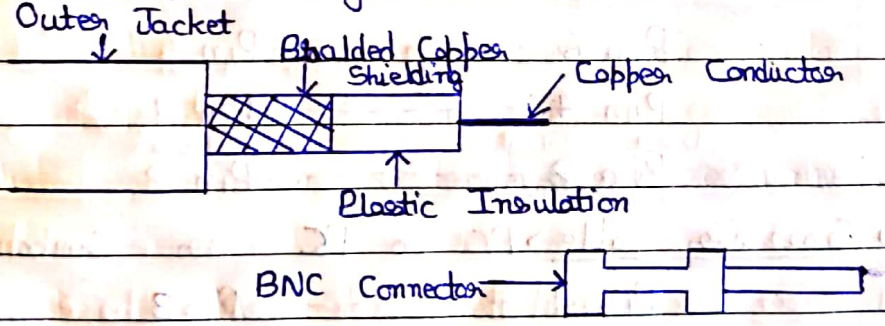
17. Cable Specifications → 10 BASE-T



Baseband Transmission	Broadband Transmission
• Baseband transmission utilizes digital signalling.	Broadband transmission uses analog signals.
• It works well with Bus & tree topologies.	It works well with Bus topology.
• It involves manchester & different manchester encoding.	It uses PSK encoding.
• The signals can be travelled in both the direction.	The signals can travel in only one direction.
• Signal can be travelled over short distances.	Signals can be travelled over long distances without being attenuated.

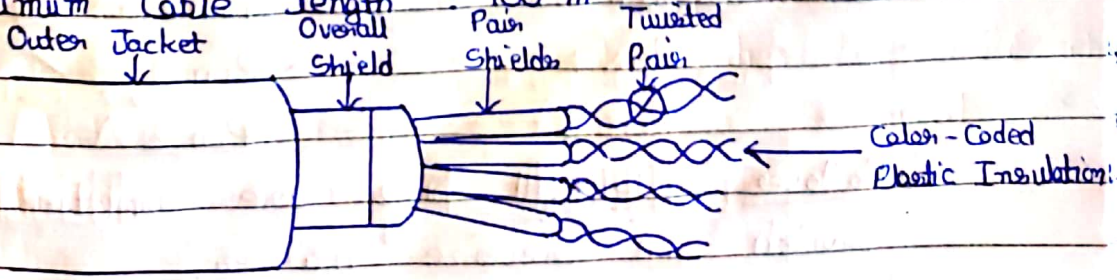
(i) Coaxial Cable → The Specifications of coaxial cable are:-

- Speed & throughput : 10 – 100 Mbps
- Average $ per node : Inexpensive
- Media & connector size : Medium
- Maximum cable length : 500 m



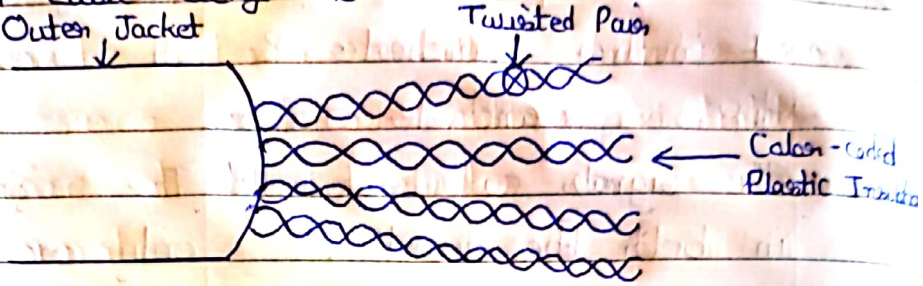
(ii) Shielded Twisted-Pair Cable → The specifications are:-

- Speed & throughput : 10 – 100 Mbps
- Average $ per node : Moderately inexpensive
- Media & connector size : Medium to large
- Maximum Cable length : 100 m



(iii) Unshielded Twisted Pair (UTP) → The specifications are:

- Speed & throughput : 10-100-1000 Mbps
- Average $ per node : Least Expensive
- Media & connector size : Small
- Maximum cable length : 100 m



(iv) Straight through Cable → To connect PC & switch. All pins are connected to corresponding switch.

Pin 1 ---------- Pin 1
Pin 2 ---------- Pin 2
Pin 3 ---------- Pin 3
Pin 4 ---------- Pin 4
Pin 5 ---------- Pin 5
Pin 6 ---------- Pin 6
Pin 7 ---------- Pin 7
Pin 8 ---------- Pin 8

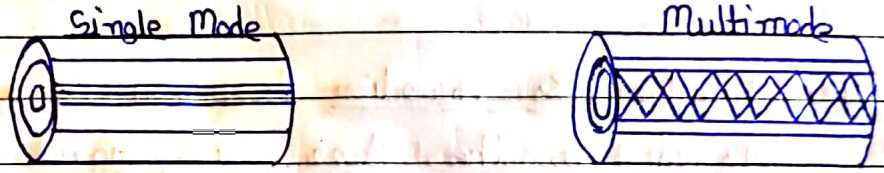
(v) Crossover Cable → PC to PC or Switch to Switch

Pin 1 ---------- Pin 3
Pin 2 ---------- Pin 6
Pin 3 ---------- Pin 1
Pin 4 ---------- Pin 4
Pin 5 ---------- Pin 5
Pin 6 ---------- Pin 2
Pin 7 ---------- Pin 7
Pin 8 ---------- Pin 8

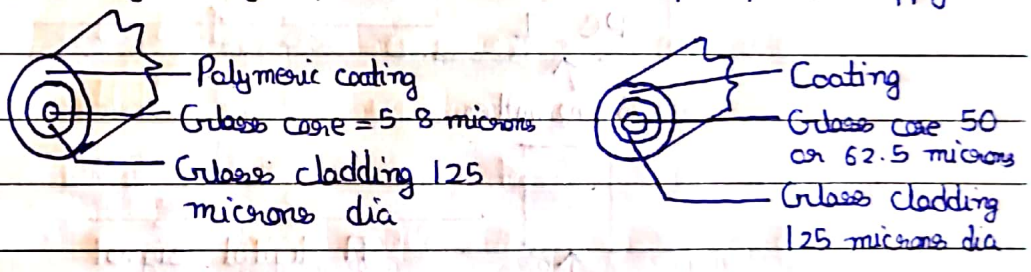
(vi) Rollover Cable → All pins are connected to corresponding switch in reverse manner.

Pin 1 ---------- Pin 8
Pin 2 ---------- Pin 7
Pin 3 ---------- Pin 6
Pin 4 ---------- Pin 5
Pin 5 ---------- Pin 4
Pin 6 ---------- Pin 3
Pin 7 ---------- Pin 2
Pin 8 ---------- Pin 1

(vii) Fibre Optic → There are two types of mode:-



Requires very straight path
Multiple paths - sloppy



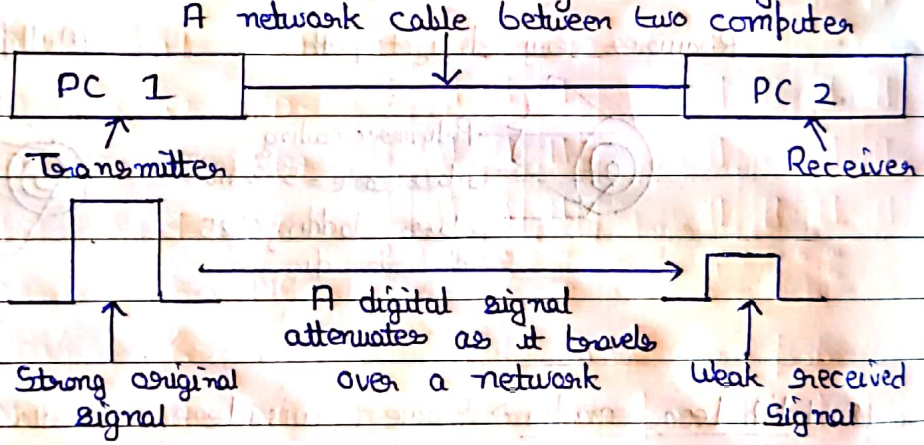
18. Wireless media → Some wireless media are:-
(i) Wireless devices (ii) PCMCIA NIC for laptops
(iii) External USB wireless NIC (iv) Access point
(v) Wireless LAN (vi) Roaming

19. Decibals → Formulas for calculating decibals:
$dB = 10 \log_{10}(P_{Final} / P_{REF})$ — Power formula
$dB = 20 \log_{10}(V_{Final} / V_{REF})$ — Voltage formula
dB is loss or gain of the power of a wave where,
P_{Final} – delivered power in watts P_{ref} – Original power in watts.
V_{Final} – delivered voltage in volts V_{ref} – Original power in voltage.

- White noise
- Narrowband interference

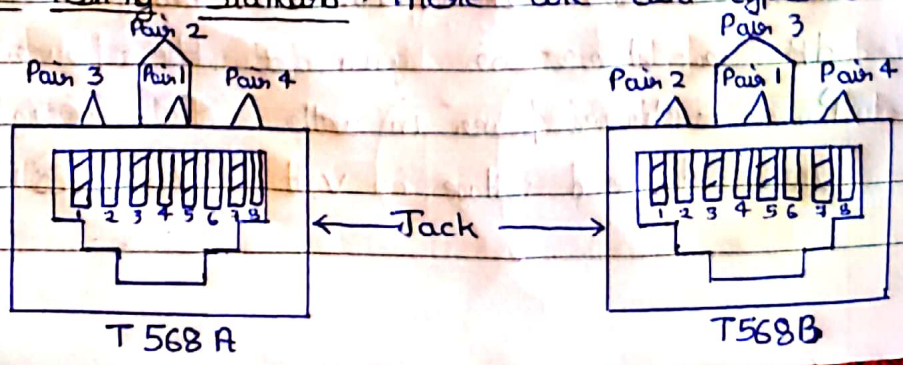
20. Noise in Time & Frequency → Noise related to communication refers to undesirable signals. Sources of noise are:
(i) Nearby cables with carry data signals.
(ii) Radio Frequency Interface (RFI), which is noise from other signals being transmitted nearby.
(iii) Electromagnetic Interface (EMI) which is noise from nearby sources such as motors & lights.
(iv) Laser noise at the transmitter or receiver of an optical signal.

21. Attenuation & Insertion loss on Copper Media → It is defined as the loss of signal / voltage.



22. Types of Crosstalk → There are three types of crosstalk.
(i) Near-end crosstalk (NEXT)
(ii) Far-end crosstalk (FEXT)
(iii) Power sum near-end crosstalk (PSNEXT)

23. Cable Testing Standard → There are two types of standard.



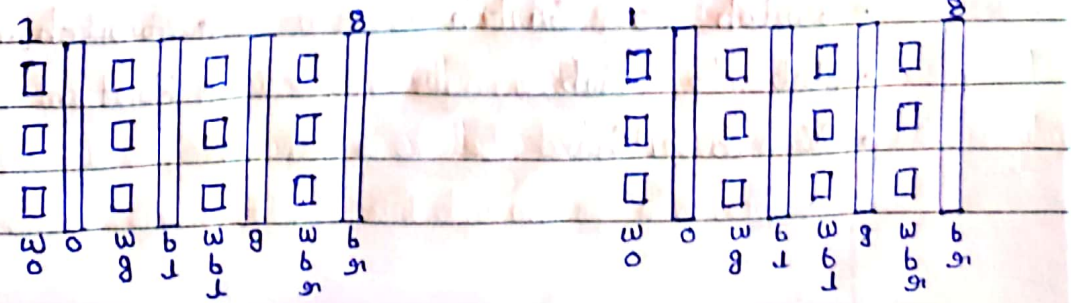
CLASSTIME	Page No.
Date	/ /

T568B	T568A
1:- Orange / White	1 :- Green White
2:- Orange	2 :- Green
3:- Green White	3 :- Orange White
4:- Blue	4 :- Blue
5:- Blue white	5 :- Blue white
6:- Green	6 :- Orange
7:- Brown white	7 :- Brown
8:- Brown	8 :- Brown white

24. LAN Physical layer Implementation → Physical layer implementation vary. Some implementations support multiple physical media. IEEE 802.2 is a standard which defines logical link control (LLC) as the upper portion of the data link layer of the OSI model.

Data link layer		Ethernet	IEEE 802.2						
Physical layer			10 BASE 2	10 BASE 5	10 BASE-T	10 BASE-F	100 BASE-TX	100 BASE-FX	1000 BASE-T
		Digital, Intel, Xerox, (DIX) Standard	802.3 Specification For 10-Mbps Ethernet	802.3 u specification for 100-Mbps (Fast) Ethernet					802.3z Specification for 1000-Mbps (Gigabit) Ethernet

25. UTP implementation - Straight - Through → Wires on cable ends are in same order



CLASSTIME	Page No.
Date	/ /

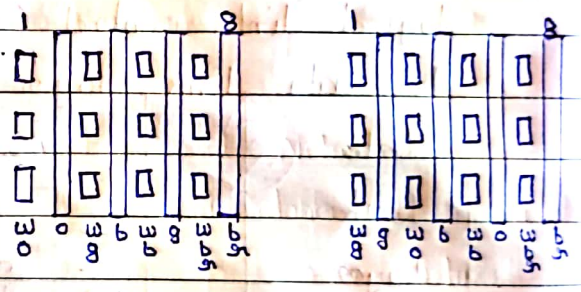
Pin	label	
1	TD+	← Transmit Data Tip +ve
2	TD-	← Transmit Data Ring -ve
3	RD+	← Receiving Data Ring +ve
4	NC	
5	NC	
6	RD-	← Receive Data Tip +ve
7	NC	
8	NC	

568 B

2.6 Interconnecting Devices using Crossover Cable →

Pin	label	Pin	label
1	TD+	1	TD+
2	RD-	2	RD-
3	RD+	3	RD+
4	NC	4	NC
5	NC	5	NC
6	TD+	6	TD-
7	NC	7	NC
8	NC	8	NC

568 B — 568 A



The orange wire pair & the green wire pair switch places on one end of the cable.

(i) Use straight-through cables for...
- Switch to router
- Switch to PC or server
- Hub to PC or server

(ii) Use roll-over cables to...
- Connect a terminal to a console port

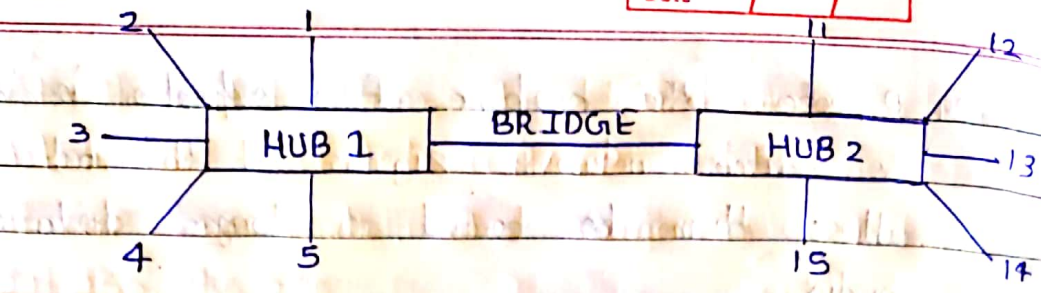
(iii) Use crossover cables for...
- Switch to Switch
- Switch to hub
- Hub to Hub
- Router to router
- PC to PC

CLASSTIME | Page No.
Date / /

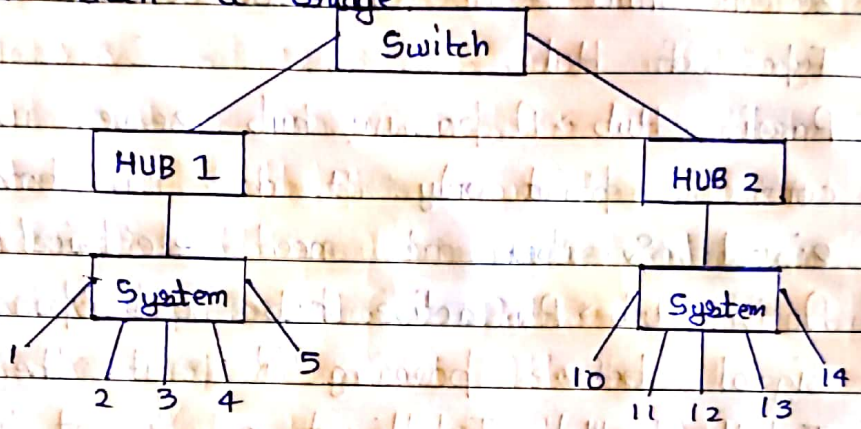
27. Repeaters → The purpose of a repeater is to regenerate & retime network signals at the bit level. This allows them to travel a longer distance on the media.

28. 8 Port Hub → Every port on a hub acts as a repeater, so the hub can also be called multiport repeater.
Types of Hub:-
(i) Passive Hub → A passive hub serves as a physical connection point only. It does not boost or clean the signal & does not need electrical power.
(ii) Active Hub → An active hub needs power to repeat the signal before passing it out the other ports.
(iii) Intelligent Hub → Intelligent or smart hubs are active hubs with a microprocessor chip & diagnostic capabilities.
The more devices there are attached to the hub, the more likely there will be collisions. Every device connected to the same network segment is said to be a member of a collision domain.

29. Bridges Segmenting a Network → The devices that are used to connect network segments together include bridges, switches, routers & gateways.
(i) Switches & bridges operate at the Data link layer of the OSI model.
(ii) If the destination address is unknown to the bridge the bridge forwards the Frame to all segments except the one on which it was received. This process is known as Flooding.



30. Switch → A switch is sometimes described as a multiple bridge. A switch is a more sophisticated device than a bridge.



31. Peer-to-Peer versus Client/Server Network →

Advantages of a Peer-to-Peer network	Advantages of a Client/Server Network
(i) Less expensive to implement.	Provides for better secu
(ii) Do not require additional specialized network administration software.	Easier to administer when the network is large because administration is centralized
(iii) Does not require a dedicated network administrator.	All data can be backed up on one central location.
Disadvantages of a Peer-to-Peer Network	**Disadvantages of a Client/Server Network**
(i) Does not scale well to large networks & administration becomes unmanageable.	Requires expensive specialized network administrative & operational software.
(ii) Each user must be trained to perform administrative tasks.	Requires expensive, more powerful hardware for the server machine

INA → Internet Naming Association

CLASSTIME | Page No.
Date / /

(iii)	Less secure.	Requires a professional administrator.
(iv)	All machines sharing the resource negatively impact the performance.	Has a single point of failure. User data is unavailable if the server is down.

32. MAC Address → The Media Access Control Sublayer is concerned with the physical components that will be used to communicate the information.
The logical link Control layer remains relatively independent of the physical equipment that will be used for the communication process.
The NIC uses the MAC address to assess whether the message should be passed onto the upper layers of the OSI model.
MAC Address : 48 bit no
Total Address : 2^{48} combinations

33. IP Address → An IP address is an identifier for a computer or a device on a TCP/IP network. There are two types of IP:-
(i) Public IP (WAN) → It is used in WAN environment.
It ranges From:-
00000000.00000000.00000000.00000000 to
11111111.11111111.11111111.11111111
i.e. 0.0.0.0 to 255.255.255.255
It contains 5 classes:-
- Class A :- Starts From 1.0.0.0 to 126.255.255.255.
- Class B :- Starts From 128.0.0.0 to 191.255.255.255.
- Class C :- Starts From 192.0.0.0 to 223.255.255.255.
- Class D :- Starts From 224.0.0.0 to 239.255.255.255.
- Class E :- Starts From 240.0.0.0 to 255.255.255.255.

IP 4 → 32-bits Size (4 octets)
IP 6 → 128-bits Size (16 octets

CLASSTIME | Page No.
Date / /

Loopback Adapter Address → It is used for checking if system has installed TCP/IP model. Checks connectivity between two hosts. Its range is 127.0.0.0 to 127.255.255.255.

(iii) Private IP (LAN) → It is used in LAN environment. It has three ranges:-

- 10.0.0.0 to 10.255.255.255 (Belongs to class A)
- 172.16.0.0 to 172.32.255.255 (Belongs to class B)
- 192.168.0.0 to 192.168.255.255 (Belongs to class C)

Private IP addresses can be reused while Public IP address is unique all over the world.

X.X.X.[0] → Network Address
X.X.X.[255] → Broadcast Address
(Not used in IP addressing)

34. Network Address Translation (NAT) → The mapping of private IP address to the public IP address of the router. This process is NAT & it's a job of the router.

35. TCP/IP Model → It has 4 layers which includes:-

(i) Application layer →

- File transfer :- TFTP → Trivial File Transfer Protocol
  FTP → File Transfer Protocol
  NFS → Network File System
- Email :- SMTP → Simple Mail Transfer Protocol
- Remote login :- Telnet, rlogin
- Network Management :- SNMP → Simple Network Management Protocol
- Name Management :- DNS → Domain Name System

(ii) Transport layer →
- Transmission Control Protocol (TCP) → Connection-oriented
- User Datagram Protocol (UDP) → Connectionless

(iii) Internet layer →
- Internet Protocol (IP)
- Internet Control Message Protocol (ICMP)
- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)

(iv) Network Access layer →
- Ethernet
- SLIP & PPP
- FDDI → Fibre Distributed Data Interface
- Proxy ARP
- Fast Ethernet
- ATM, Frame relay & SMDS
- ARP
- RARP

36. TCP / IP vs OSI

TCP / IP Model		OSI Model	
Application	Protocols	Application Presentation Session	Application Layer
Transport		Transport	
Network		Network	Data Flow Layers
Network Access	Networks	Data Link Physical	

37. IP addressing & classes

IP Address class	High Order Bits	First Octet Address Range	Number of Bits in the Network Address
Class A	0	0-127	8
Class B	10	128-191	16
Class C	110	192-223	24
Class D	1110	224-239	28

Class A	Network	Host		
Octet	1	2	3	4
Class B	Network		Host	
Octet	1	2	3	4
Class C	Network			Host
Octet	1	2	3	4
Class D	Host			
Octet	1	2	3	4

Network → It is a collection of Host

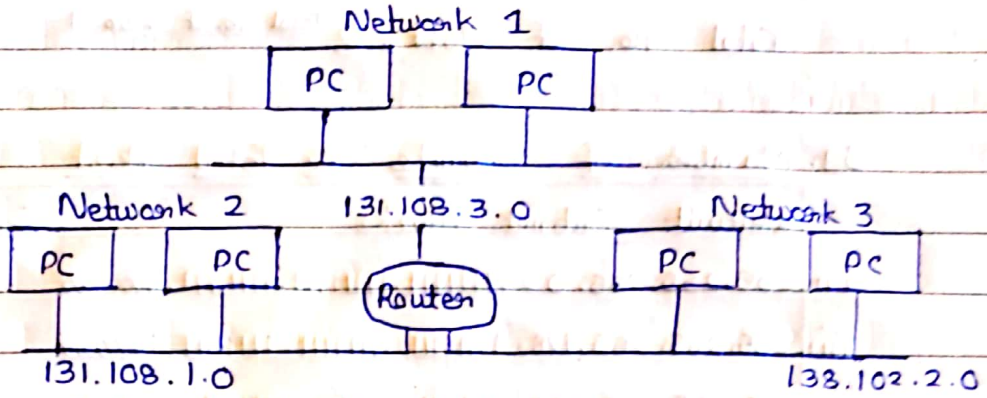
Host → Single Computer

Ex:- 192.168.6.1 } The collection of IP will be
192.168.6.254 } assigned to the Computer on a LAN
Network Host

220.67.131.5 } These are the IP addresses
220.67.131.50 } alloted to WAN environment
Network Host } to the routers on a public IP

38. Subnetting → It is the practice of dividing a network into two or more smaller network. It increases routing efficiency, enhances the security of the network & reduces the size of broadcast domain

Decimal notation for First Host octet	No. of Subnets	No. of class A Host / Subnet	No. of class B Hosts/Subnet	No. of class C Hosts/Subnet
192	2	4,194,302	16,382	62
224	6	2,097,150	8,190	30
240	14	1,048,574	4,094	14
248	30	524,286	2,046	6
252	62	262,142	1,022	2
254	126	131,070	510	-
255	254	65,534	254	-



Reasons For Subnetting:-

(i) Provides addressing Flexibility for the network administrator.

(ii) Provides broadcast containment & low-level security on the LAN.

(iii) Provides some security since access to other subnets is only available through the services of a router.

Class	Default Subnet Mask
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

If we do logical AND on default subnet mask with Packet address (IP), we get the subnetwork address or packet address. Ex:-

(i)	Packet Address	192.168.10.65	11000000.10101000.00001010.01000001
	Subnet Mask	255.255.255.224	11111111.11111111.11111111.11100000
	Subnetwork address	192.168.10.64	11000000.10101000.00001010.01000000
(ii)	Packet Address	192.168.1.56	11000000.10101000.00000001.00111000
	Subnet Mask	255.255.255.128	11111111.11111111.11111111.10000000
	Subnetwork Address	192.168.1.0	11000000.10101000.00000001.00000000
(iii)	Packet Address	192.168.1.0	11000000.10101000.00000001.00000000
	Subnet Mask	255.255.255.0	11111111.11111111.11111111.00000000
	Subnetwork Address	192.168.1.0	11000000.10101000.00000001.00000000

Total no. of Subnets = 2^N (N = No. of bit changed)

CLASSTIME | Page No.
Date / /

Total no. of Host = $2^{\text{Total no. of zeros}} - 1$

39. Number of Subnets & Total Host

	Default Subnet Masks	Subnets	Hosts
(i)	255.255.255.0 = 11111111.11111111.11111111.00000000	1	256
(ii)	255.255.255.128 = 11111111.11111111.11111111.10000000	2	128
(iii)	255.255.255.192 = 11111111.11111111.11111111.11000000	4	64
(iv)	255.255.255.224 = 11111111.11111111.11111111.11100000	8	32
(v)	255.255.255.240 = 11111111.11111111.11111111.11110000	16	16
(vi)	255.255.255.248 = 11111111.11111111.11111111.11111000	32	8
(vii)	255.255.255.252 = 11111111.11111111.11111111.11111100	64	4
(viii)	255.255.255.254 = 11111111.11111111.11111111.11111110	128	2

- Range For (i) having IP 192.168.1.0 is (192.168.1.0 - 192.168.1.255)
  Subnet ID Subnet Broadcast ID
  By convention, these are not assign to any person
  Total usable Subnet range is
  (192.168.1.1 - 192.168.1.254) Hosts = 254
- Range For (ii) having IP 192.168.1.0 is
  (i) (192.168.1.0 - 192.168.1.127)
  Subnet ID Subnet Broadcast ID
  Total usable range is
  (192.168.1.1 - 192.168.1.126) Host = 126
  (ii) (192.168.1.128 - 192.168.1.255)
  Subnet ID Subnet Broadcast ID
  Total usable range is
  (192.168.1.129 - 192.168.1.254) Host = 126
- Range For (iii) having IP is 192.168.1.0 is
  (i) (192.168.1.0 - 192.168.1.63)
  Total usable range is

CLASSTIME | Page No.
Date / /

(192.168.1.1 - 192.168.1.62) Hosts = 62

(ii) (192.168.1.64 - 192.168.1.127)

Total usable range is

(192.168.1.65 - 192.168.1.126) Hosts = 62

(iii) (192.168.1.128 - 192.168.1.191)

Total usable range is

(192.168.1.129 - 192.168.1.190) Hosts = 62

(iv) (192.168.1.192 - 192.168.1.255)

Total usable range is

(192.168.1.193 - 192.168.1.254) Hosts = 62