Subject Code	Subject Name	Teaching Scheme (Hrs.)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Practical	Tutorial	Total
ECC602	Computer Communication Networks	04	--	--	04	--	--	04

Subject Code	Subject Name	Examination Scheme							
		Theory Marks				Term Work	Practical & Oral	Oral	Total
		Internal assessment			End Sem. Exam				
		Test 1	Test2	Avg. Of Test 1 and Test 2					
ECC602	Computer Communication Networks	20	20	20	80	--	--	--	100

Course Pre requisite:

- AnalogCommunication

Course objectives:

- To introduce analysis and design of computer and communication networks.
- To design and configure a network for an organization. To implement client-server socket programs.
- To analyse the traffic flow and the contents of protocolframes.

Course outcomes:

After successful completion of the course student will be able to

- Design a small or medium sized computer network including media types, end devices,and interconnecting devices that meets a customer's specificneeds.
- Perform basic configurations on routers and Ethernet switches.
- Demonstrate knowledge of programming for networkcommunications.
- Learn to simulate computer networks and analyse the simulationresults.
- Troubleshoot connectivity problems in a host occurring at multiple layers of the OSImodel.
- Develop knowledge and skills necessary to gain employment as computer network engineer and network administrator.

Module No.	Unit No.	Topics	Hrs.
1.0		**Introduction**	06
	1.1	Network Applications	
	1.2	Network Hardware	
	1.3	Network Software	
	1.4	Reference Models, overview of TCP/IP, layer Functions, services, sockets and ports, Encapsulation.	
2.0		**Introduction to Physical layer Services and System**	08
	2.1	Introduction to physical media, Coax, RJ 45 , fiber, twisted pair, DSL, HFC, WiMax, cellular, satellite, and telephone networks, bit transmission, frequency division multiplexing. time division multiplexing.	
3.0		**The Data Link Layer**	08
	3.1	Data link Layer Design Issues	
	3.2	Error Detection and Correction	
		Elementary Data Link Protocols, Sliding Window Protocols	
		Example Data Link Protocols: HDLC: High-Level Data Link Control, The Data Link Layer in The Internet.	
4.0		**The Medium Access Sub- Layer**	06
	4.1	Channel Allocation Problem.	
	4.2	Multiple Access Protocols.	
5.0		**The Network Layer**	10
	5.1	Network Layer Design Issues.	
	5.2	Routing Algorithms.	
	5.3	Congestion Control Algorithms, Quality of Service.	
	5.4	Internetworking.	
	5.5	The Network Layer In The Internet: The IP Protocol, IPv4 header, IP Addressesing, Subnetting.	
	5.6	Internet Control Protocols, The Interior Gateway Routing Protocol: OSPF, The Exterior Gateway Routing Protocol: BGP.	
6.0		**The Transport Layer**	10
	6.1	The Transport Service.	
	6.2	Elements of Transport Protocols.	
	6.3	The Internet Transport Protocol: UDP	
	6.4	The Internet Transport Protocol: TCP:-Introduction to TCP, The TCP Service Model, The TCP Protocol.	
	6.5	The TCP Segment Header.	
	6.6	TCP Connection Establishment, TCP Connection Release.	
	6.7	Modeling TCP Connection Management.	
	6.8	TCP Transmission Policy.	
	6.9	TCP Congestion Control.	
	6.10	TCP Timer Management, Transactional TCP.	

		Total	48

Text Books:

1. A. S. Tanenbaum,‖Computer Networks‖, 4th edition, PrenticeHall
2. B. F. Ferouzan,‖Data and Computer Communication‖, Tata McGrawHill.

Reference Books:

1. Peterson&Davie, -ComputerNetworks‖, 2nd Edition, Morgan Kaufmann.
2. Kurose, Ross, —Computer Networking‖, AddisonWesley
3. S. Keshav,-An Engg, Approach To ComputerNetworking‖, AddisonWesley.
4. W. Richard Stevens, —TCP/IP Volume1, 2, 3‖, AddisonWesley.
5. D.E.Comer, -Computer Networks AndInternets‖, PrenticeHall.
6. B. F.Ferouzan , -TCP/IP Protocol Suite‖, Tata McGrawHill.

Internal Assessment:
Assessment consists of two class tests of 20 marks each. The first class test is to be conducted when approximately 40% syllabus is completed and second class test when additional 40% syllabus is completed. The average marks of both the test will be considered for final Internal Assessment. Duration of each test shall be of one hour.

End Semester Examination:
1. Question paper will comprise of 6 questions, each carrying 20marks.
2. The students need to solve total 4questions.
3. Question No.1 will be compulsory and based on entiresyllabus.
4. Remaining question (Q.2 to Q.6) will be selected from all themodules.

Chapter 1: Introduction

1.1 Network Applications
1.2 Network Hardware
1.3 Network Software
1.4 Reference Models, overview of TCP/IP, Layer Functions, Services, Sockets and ports, Encapsulation

1.1. Network Applications

① Business Applications
1) Resource sharing
- storage sharing
- Printer sharing

2) Virtual Private Networks (e.g. Reliance Jio or tata comm n/w can be accessed by their employees from here)

3) Client Server Model (e.g. siesget n/w)
[e.g. All students, faculty, non-teaching, administrative staff sharing the storage (Z_drive)]

4) Web Application

5) Email

6) VoIP

7) Desktop sharing (Teamviewer)

8) e-Commerce (e.g. Amazon web Store) Airlines etc.

9) Sharing of Google Docs, google sheets, google classroom etc

② Home Applications

- Internet Access on home PC
- www.ieee.org
- Social n/w → facebook
  - → Wikipedia
  - → Twitter
- IPTV
- Youtube

③ Mobile Users

- Read and send email
- Tweet
- Watch movies
- download music
- Play games
- Surf Web
- Wireless hotspots — 802.11
- GPS

II Network Hardware

- Transmission Technology
  - → Broadcast Links
  - → Point-to-point (P2P Links, Unicasting)
  - → Multicast links
  - → Anycast links
- Personal Area Networks
  - → Bluetooth
  - → PC with its peripherals
- Local Area Networks
- Metropolitan Area Networks
- Wide Area Networks

III Network Software

- protocol Hierarchies
- Layered Models.

Reference Models

① TCP/IP ~~Model~~ or Architecture OR TCP/IP protocol Suite
Transmission control protocol / Internet protocol

② ISO OSI Models
International Standards organization Open System Interconnection Model.

- Detailed notes on TCP/IP and OSI in other notebook (IVC)

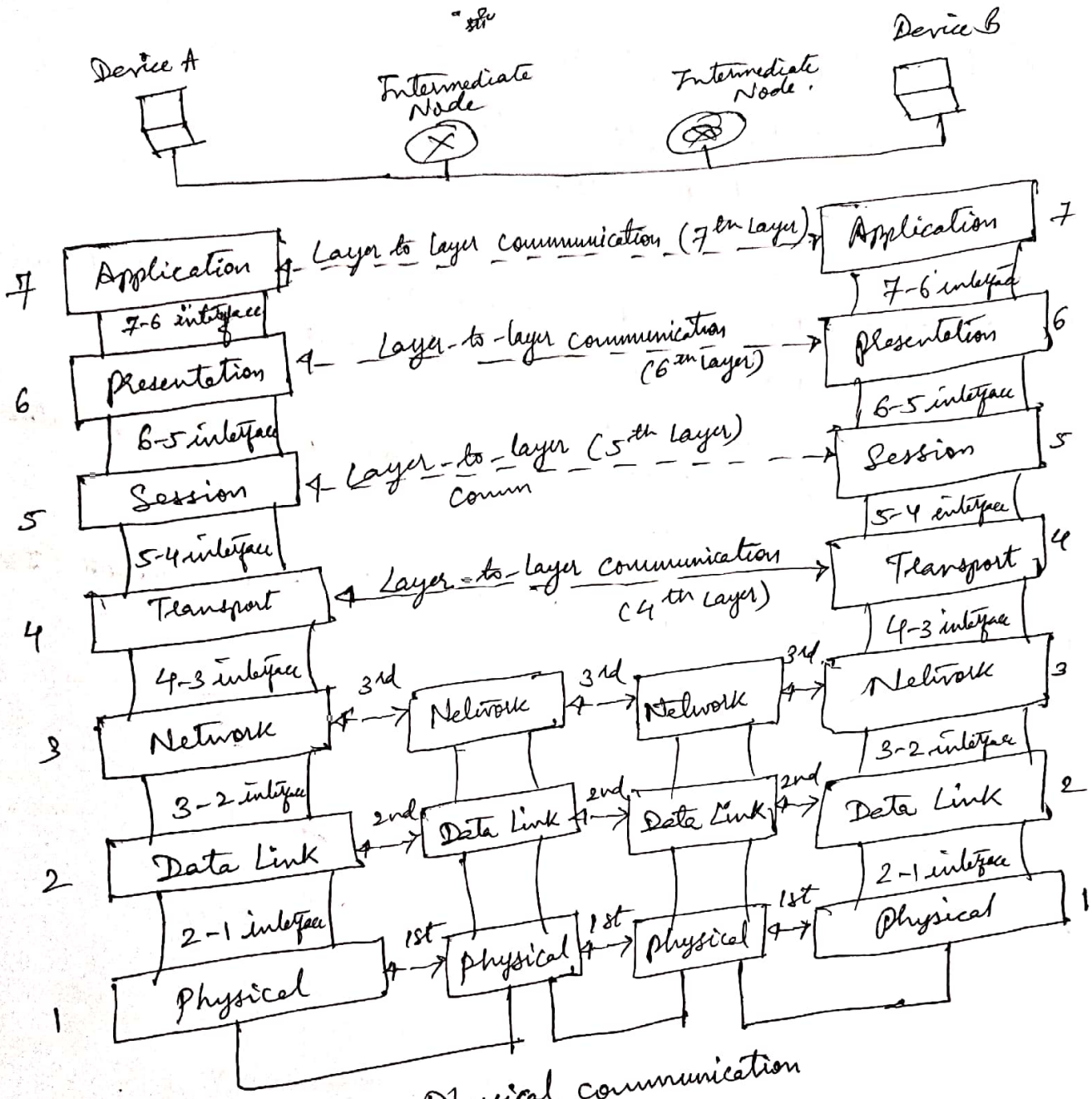


Fig: OSI Layers (OSI communication model)

Q. Draw and Explain OSI reference model with functions of each layer, devices (H/w devices) used at each layer, data format at each layer, address at each layer and protocols at each layer.

Layers		Functions
L7	Application	Allows Network access to user, Email access Remote Login, WWW access ----
L6	Presentation	Data Translation, Encryption, decryption, Compression, decompression
L5	Session	Establish, maintain & release connections login & logout time, Inserts check points in large size files, dialogue control
L4	Transport	Reliable byte stream communication, multiplexing & demultiplexing, port addressing, flow control, Error control congestion control
L3	Network	Addressing, routing, congesting control
L2	Data Link	Flow control, medium access control framing, Error control, Hardware addressing
L1	Physical	Line Encoding, Transmission rates Physical topologies, Bits, Mode of communication (Simplex, half duplex full duplex) Electrical & Mechanical aspects of comm.

OSI Model

* Communication stack is present as software in operating system (But OSI Model is not implemented TCP/IP architecture is part of operating system)

	Data Formats	Hardware Devices	Address	Mode of Communication
Application	Application Layer Protocol data unit (ALPDU)	Gateways	Socket Address	End to End
Presentation	Presentation Layer protocol data unit (PLPDU)	Gateways		
Session	Session Layer protocol data unit (SLPDU)	Gateways		
Transport	Segments or Datagrams or Packets	Gateways, Brouter	Port address	Process to process
Network	Packets or Datagrams	Router	Logical address (IP address)	Source to destination
Data Link	Frames	Switch, Bridge	MAC address (Hardware address, link address, physical address)	Node to Node or Hop by Hop
Physical	Bits	Repeaters, Hubs, amplifiers, oscillators		Node to Node or Hop by Hop

OSI Model

At Transport layer

Segments is the Data format when TCP protocol is used

Datagrams is the Data format when UDP protocol is used

Packets is the Data format when SCTP protocol is used.

Datagrams are small size packets (packets are broken down into datagrams)

Protocols

Application	HTTP, FTP, TFTP, DNS, TELNET, SSH, DHCP, RLogin, SMTP
Presentation	MIME, TLS, SSL
Session	CHAP, PAP, Network file systems (NFS), NetBIOS
Transport	TCP, UDP, SCTP, DCCP
Network	IP, RIP, OSPF, BGP, EIGRP, IGMP, ICMP
Data Link	HDLC, LAPD, PPP
Physical	IEEE 802.3, IEEE 802.11

Network Basic I/p O/p System

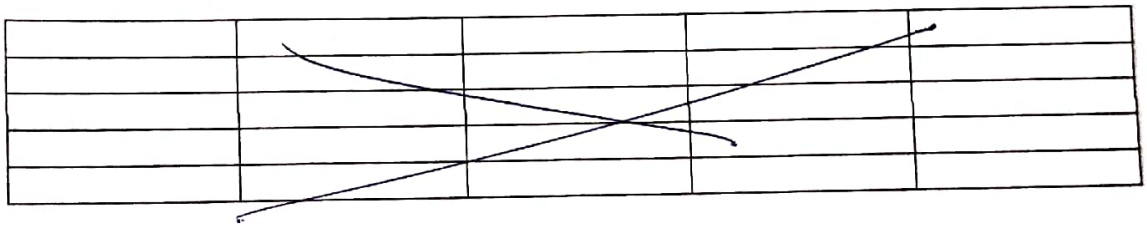
1. Introduction to TCP/IP:
TCP/IP networking model, layer functions, TCP/IP protocols, services, sockets and ports, encapsulations, differences between ISO and internet layering

Layers	Functions	Data Format	Protocols	Services	Hardware component
Application	application specific	Application layer protocol data unit	Ping,traceroute,Telnet, FTP, E-mail(SMTP), WWW,bootp,tftp,snmp,mftp	provide network access to application programs	Gateway
Presentation	1.Data translation(syntax& semantics) 2.Encoding 3.Compression & Decompression 4.Encryption & Decryption	presentation layer protocol data unit	ASN.1, ISO presentation protocol	handle compatibility issues	Gateway
Session	1.Authentication 2.Session establishment & release(session management) 3.Insert checkpoints 4.Dialogue control 5.Recovery	Session layer protocol data unit	ISO session protocol, RPC	support communication between cooperating application programs	Gateway
Transport	1.Multiplexing / Demultiplexing 2.Fragmentation and Re-assembly 3.Types of service 4.Error Control 5.Flow Control 6.Connection Establishment / Release	Segments	TCP, UDP, ISO TP0 - TP4	control delivery of messages between hosts	Gateway
Network	1.Routing 2.Switching 3.Addressing 4.Congestion Control 5.Internetworking	Packets	IP, X.25, CLNP,ICMP,IGP,IGRP,OSPF,BGP	Provide switching and routing functions to transfer data between hosts	router
Data Link	1.Framing 2.Acknowledgment 3.Sequence Numbering 4.Error Detection 5.Retransmission 6.Flow Control	Frames	HDLC, CCITT, LAP-D	Reliable transfer of frames over a link	Switches, bridges
Physical	1.Hardware Specification 2.Encoding and Signaling 3.Data	Bits	X.21, RS-232-C	Transmission of a raw bit stream over a communication channel ensuring	Repeater, hub

Physical Layer (contd.)	Transmission & Reception 4.Topology& Network Design 5.Conversion of bits into electrical or optical signals			a reliable delivery of 0's and 1's	

TCP/IP networking model:

Application	Application
	Presentation
	Session
Transport	Transport
Network(Internet)	Network
Host-to-Network	Data Link
	Physical
TCP/IP Model	**OSI Model**



differences between ISO and internet layering

OSI	TCP/IP
Application (Layer 7)	Application Layer
Presentation (Layer 6)	
Session (Layer 5)	
Transport (Layer 4)	Transport Layer
Network (Layer 3)	Internet(Network)
Data Link (Layer 2)	Subnet(Host-To-Network)
Physical (Layer 1)	

OSI	TCP/IP
Approaches of the Application layer to construct application entities is different Than that of corresponding layer in TCP/IP model	Approaches of the Application layer to construct application entities is different Than that of corresponding layer in OSI model
Session Layer Present	Session Layer not Present, its characteristics are provided by the TCP protocol. (Transport Layer)
Presentation Layer Present	Presentation Layer not Present, its function is provided by the Application Layer.
In OSI the transport layer uses the terms 'connection oriented' and 'connectionless' for the connection and connectionless models respectively.	In TCP/IP the transport layer uses the terms 'connections' and 'datagrams' for the connection and connectionless models respectively.
The network layer provides both connectionless and connection-oriented services.	The internet layer is exclusively connectionless.
Strictly Layered	Loosely Layered
Does not support internetworking	supports internetworking
Model was devised first and then the protocols were invented	

OSI LAYERS

7 Application	HTTP, SMTP, SNMP, FTP, Telnet, SIP, SSH and Scp, NFS, RTSP, Feed, Webcal, XMPP, Whois, AppleTalk, Print Services
6 Presentation	XDR, ASN.1, SMB, AFP, NCP
5 Session	TLS, SSH, ISO 8327 / CCITT X.225, RPC, NetBIOS, ASP, Winsock, BSD sockets CHAP PAP
4 Transport	TCP, UDP, RTP, SCTP, SPX, ATP DCCP
3 Network	IP, ICMP, IGMP, BGP, OSPF, RIP, IGRP, EIGRP, ARP, RARP, X.25
2 Data Link	Ethernet, Token ring, HDLC, Frame relay, ISDN, ATM, 802.11 WiFi, FDDI, PPP
1 Physical	wire, radio, fiber optic, Carrier pigeon

TCP Layers

4 Application (OSI layers5 through 7) HTTP, FTP, DNS
(Routing protocols like BGP and RIP, which for a variety of reasons run over TCP and UDP respectively, may also be considered part of the Internetwork layer)

3 Transport (OSI layers4 and 5) TCP, UDP, RTP, SCTP
(Routing protocols like OSPF, which run over IP, may also be considered part of the Internetwork layer)

2 Internetwork (OSI layer 3) For TCP/IP this is the Internet Protocol (IP)
(Required protocols like ICMP and IGMP run over IP, but may still be considered part of the Internetwork layer; ARP does not run over IP)

1 Link (OSI layers 1 and 2) Ethernet, Wi-Fi, MPLS, etc.

Shubhangi Kharche

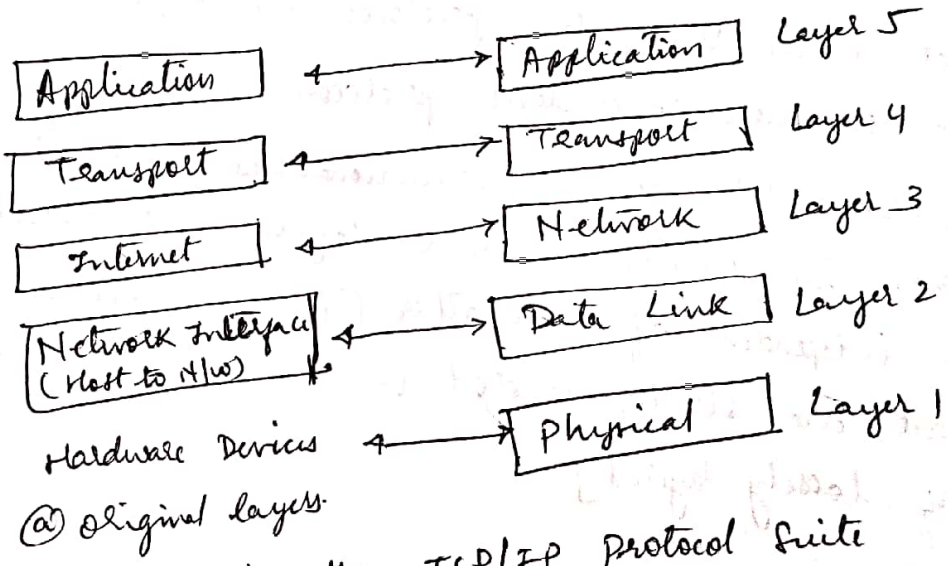
Module No 1. Review of TCP/IP

1.1 TCP/IP networking Model, layer Functions
1.2 TCP/IP protocols, services, sockets and ports, encapsulations, difference between ISO and Internet layering

1.1 TCP/IP networking model

TCP/IP protocol suite:

- It was developed prior to the OSI model.
- It has four software layers built upon the Hardware.
- Its now called a 5-layer model.

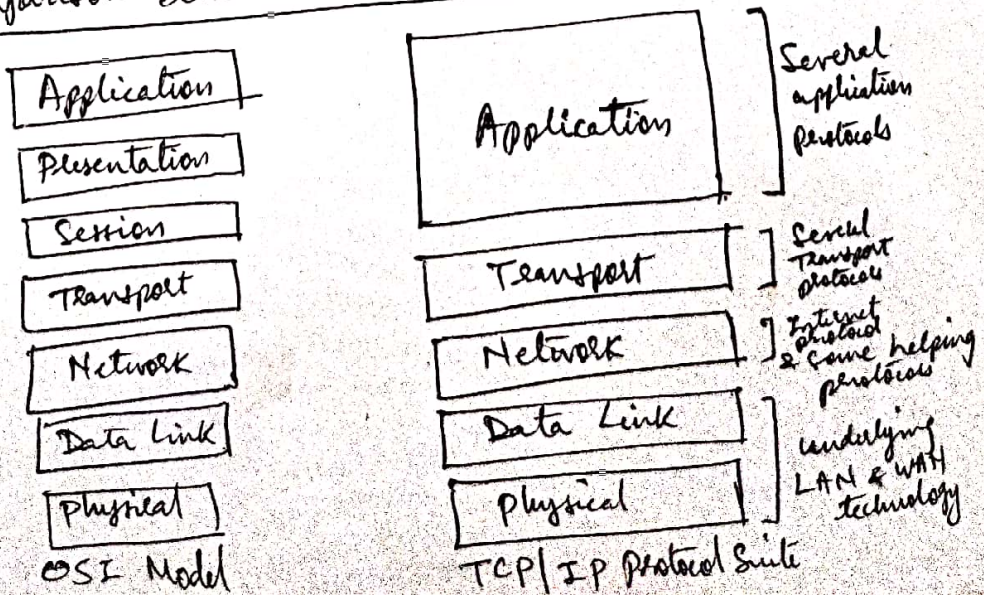


@ original layers.

fig 1: Layers in the TCP/IP protocol suite

Comparison Between OSI & TCP/IP protocol suit

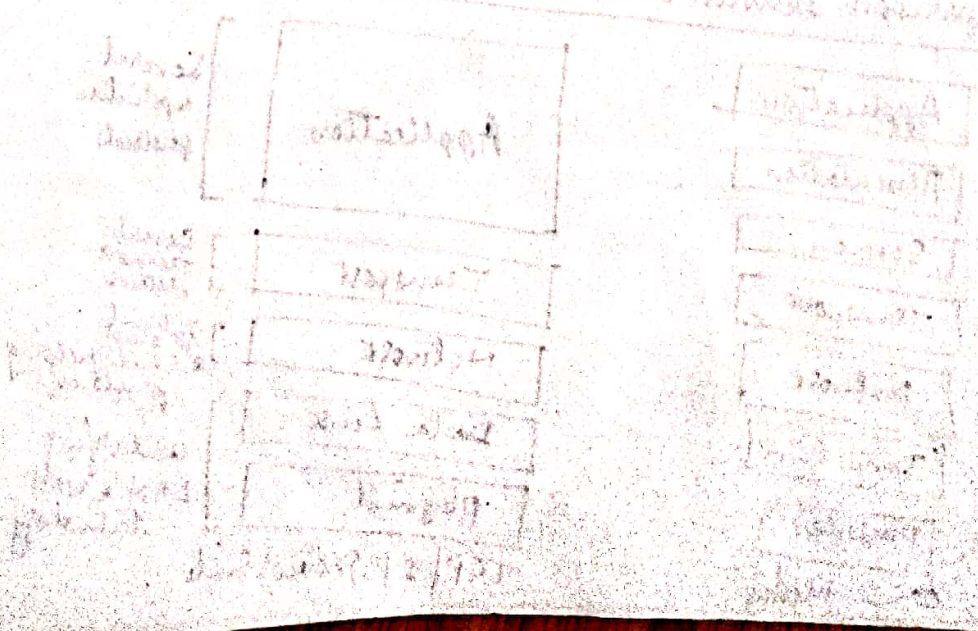
fig 2:



- Session & presentation layers are missing in TCP/IP protocol suite.
- The application layer in TCP/IP protocol suite = appl^n layer + Session layer + presentation layers.
- Some of the functionalities of the session layer are available in some of the transport layer protocols.
- And some of the functionalities of the session layer & presentation can be developed along with the piece of SW at the appl^n layer.
- TCP/IP protocol architecture is hierarchical, means that each upper level protocol is supported by one or more lower level protocols.

: In OSI model layerwise functionalities are fixed whereas in TCP/IP model layerwise functionalities are independent of each other [i.e. layers in OSI model are strictly layered whereas layers in TCP/IP are loosely layered]

Layers in:



Layers in the TCP/IP Protocol Suit

Links:

- Connect computers, routers, switches together in a n/w.
- may be Satellite links, μWave links, coaxial cables, Straight through cables, crossover cables, Rollover cables, optical fibre cables.

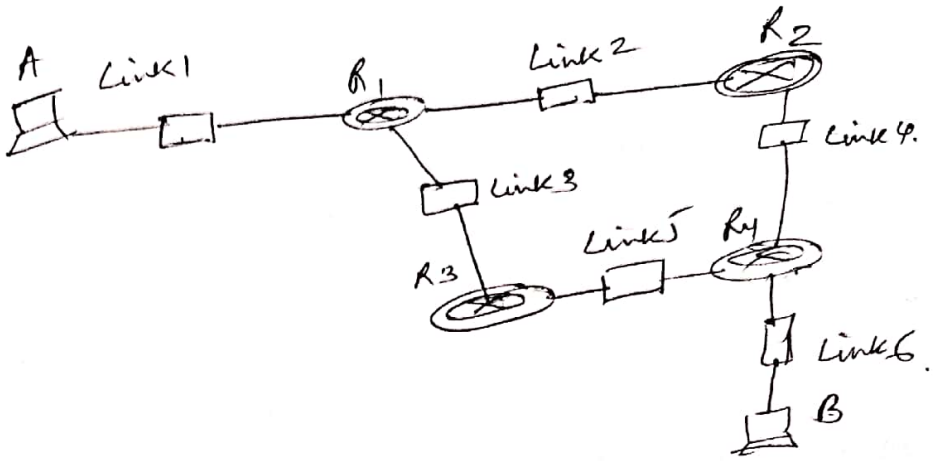
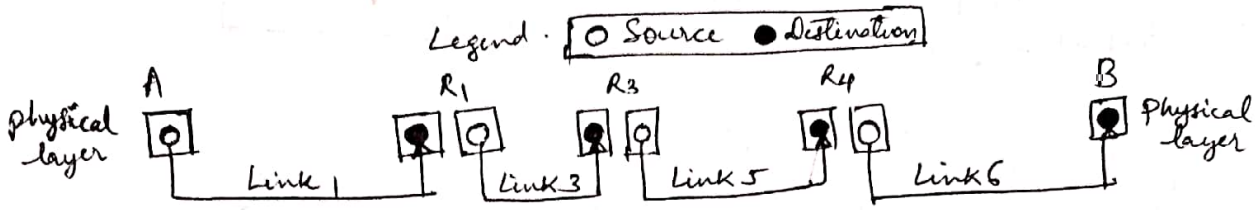


fig3: A private internet

Physical Layer:

- No specific protocol at physical layer.
- It supports all standard & proprietary protocols.
- At this layer level, the communication is between two hops or nodes, either a computer or router.
- The unit of communication is a bit.
- When the communication is established between the two nodes, a stream of bits is flowing between them.
- Physical layer treats each bit individually.



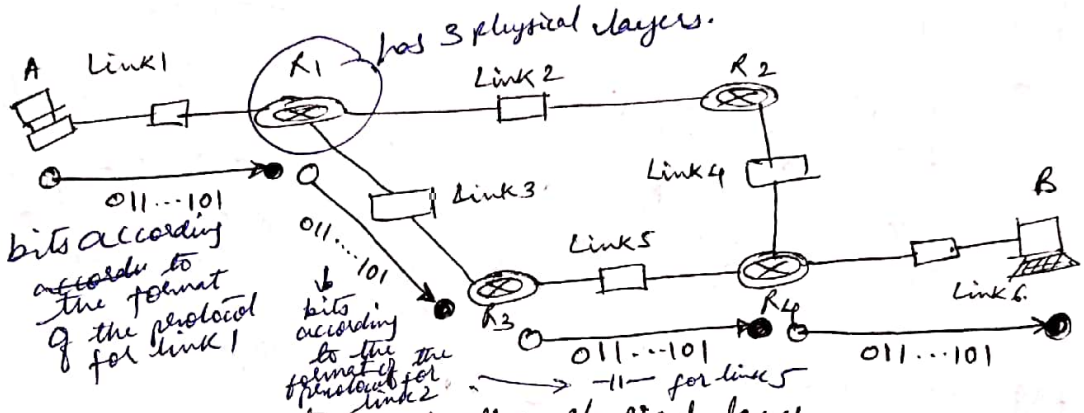


fig: Communication at the physical layer.

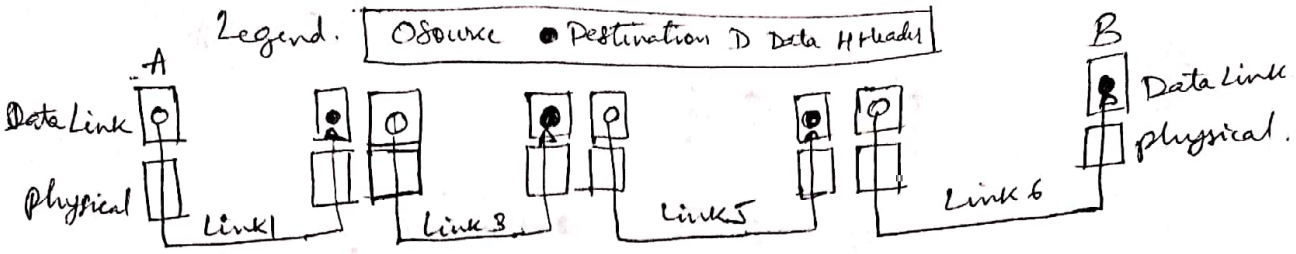
Each computer involves one Link
Each Router involves two links
n physical layer protocols are needed for n links

Wired LAN Protocol - IEEE 802.3 → Ethernet

Wireless LAN Protocol - IEEE 802.11, Bluetooth → IEEE 802.15.1
↓
wireless Ethernet

Data Link Layer:

- No specific protocol for data link layer.
- Comm is bet^n two hops or nodes.
- Unit of comm is frame
- A frame is a packet that encapsulates the data received from the network layer with an added header & sometimes a trailer.
- Header has source & destination address for a frame:
- Destination addr defines the receipient
- Source addr is needed for sending ack.



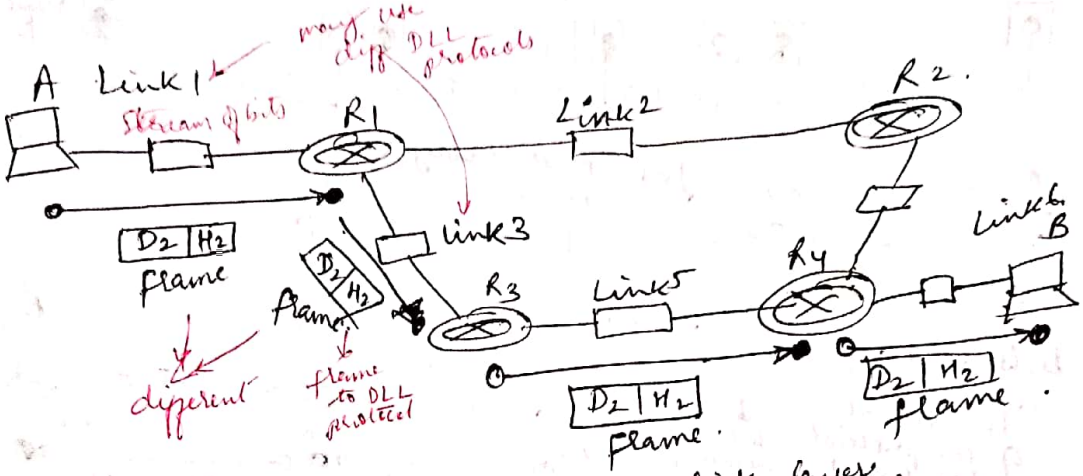


fig 5: Communication at the data link layer.

Network Layer:

- At n/w layer (or internetwork layer), TCP/IP supports the Internet protocol (IP).
- The Internet protocol (IP) is the transmission mechanism used by the TCP/IP protocols.
- IP transports data in packets called datagrams, each of which is transported separately.
- Datagrams can travel along different routes and can arrive out of sequence or be duplicated.
- IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

Difference between the communication at the n/w layer & the comm at data link & physical layers:

- At n/w layer comm is end to end
- At DLL comm is node to node
- At physical layer comm is node to node.

Shubhangi K

- The datagram started at computer A is the one that reaches computer B.
- The network layers of the routers can inspect the source & destination of the packet for finding the best route, but they are not allowed to change the contents of the packet.
- Of course, the communication is logical, not physical.
- Although the n/w layer of computer A and B think that they are sending & receiving datagrams, the actual communication again is done at the physical level.
- The unit of communication at the network layer is a datagram:

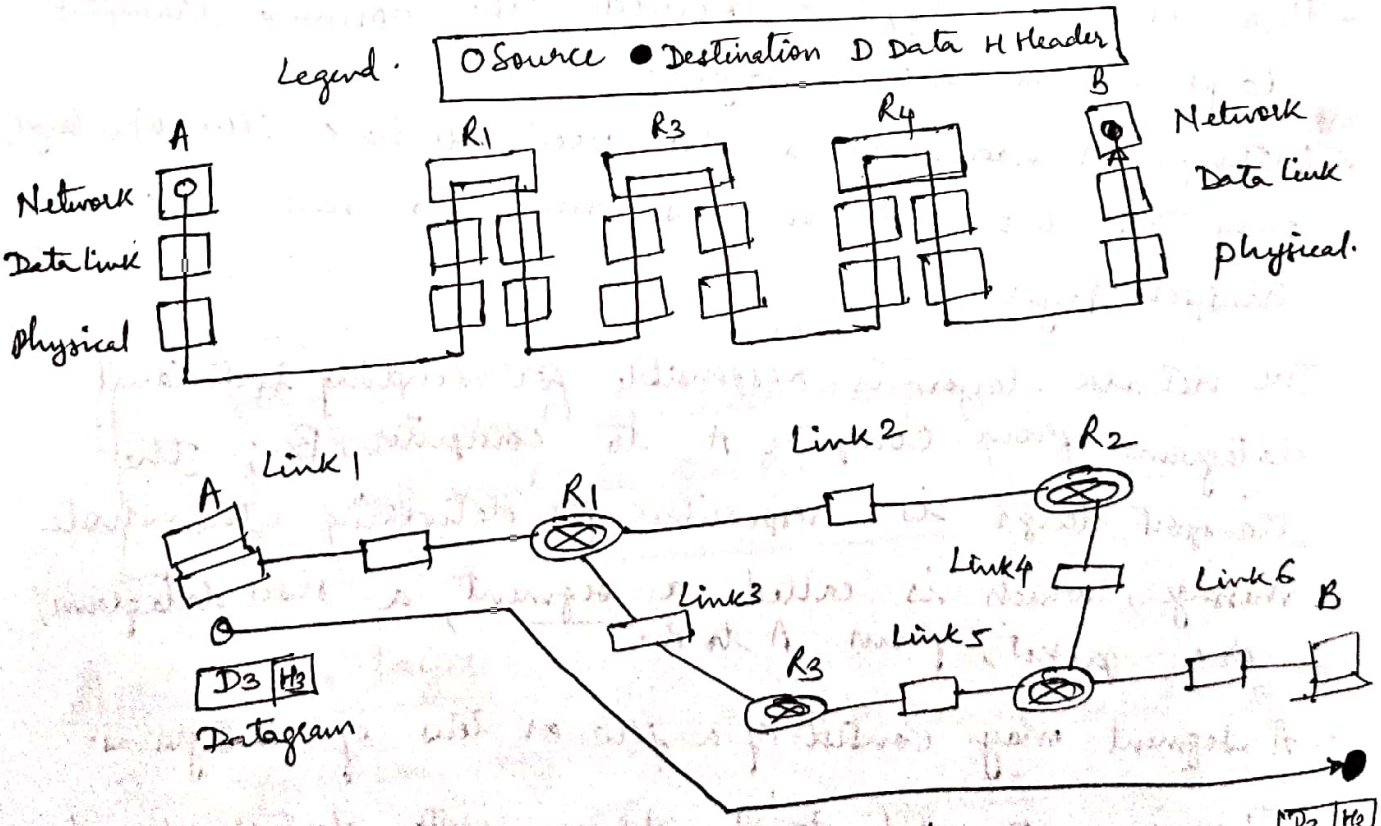


fig 6: Communication at the network layer.. (Source to destination) or (End to End)

Transport
Application Layer

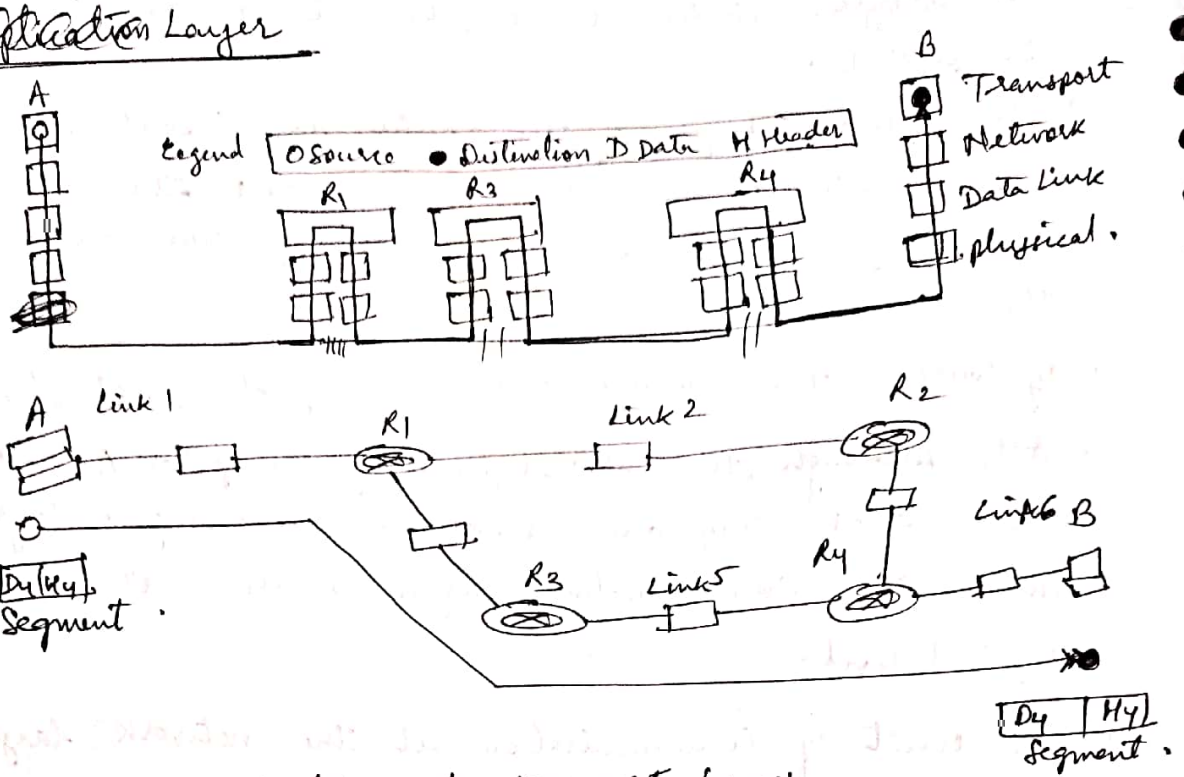


fig7: Communication at transport Layer.

- There is a main difference between the transport layer & the network layer.
- Although all nodes in a n/w need to have the n/w layer, only the two end computers need to have the transport layer.
- The network layer is responsible for sending individual datagrams from computer A to computer B; the transport layer is responsible for delivering the whole message, which is called a segment, a user datagram, or a packet, from A to B.
- A segment may consist of a few or tens of datagrams.
- The segments need to be broken into datagrams and each datagram has to be delivered to the network layer for transmission.
- Since the Internet defines a different route for each datagram, the datagrams may arrive out of order & may be lost.

- The transport layer at computer B needs to wait until all of these datagrams to arrive, assemble them and make a segment out of them.
- Again, we should know that the two transport layers only think that they are communicating with each other using a segment; the communication is done through the physical layer & the exchange of bits.
- Traditionally, the transport layer was represented in the TCP/IP suite by two protocols: user Datagram protocol (UDP) and Transmission Control protocol (TCP). A new protocol called Stream Control Transmission protocol (SCTP) has been introduced in the last few years.
- The Unit of Communication at the transport layer is a segment, user datagram, or a packet, depending on the specific protocol used in this layer.

for TCP unit is Segment
for UDP unit is User datagram
for SCTP unit is packet

Application Layer

- The application layer in TCP/IP is equivalent to the combined Session, Presentation and application layers in the OSI model.
- The application layers allows a user to access the services of our private internet or the global internet.

- Many protocols are defined at this layer to provide services such as electronic mail, file transfer, accessing the World Wide Web & so on.
- Note that the communication at the application layer, like the one at the transport layer, is end to end.
  - A message generated at computer A is sent to computer B without being changed during the transmission.
- The unit of communication at the application layer is a message.

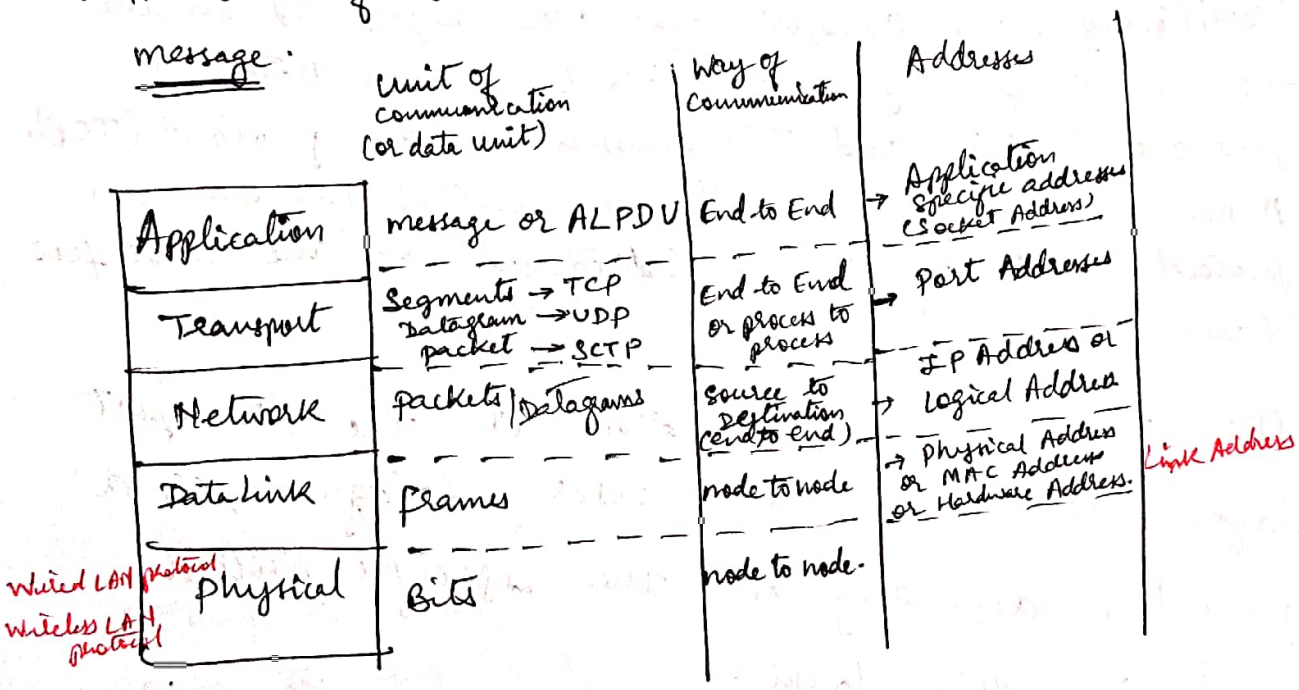


fig: TCP/IP Stack

ALPDU: Application layer protocol Data Unit

TCP: Transmission Control protocol

UDP: User Datagram protocol

SCTP: Stream Control Transmission Protocol.

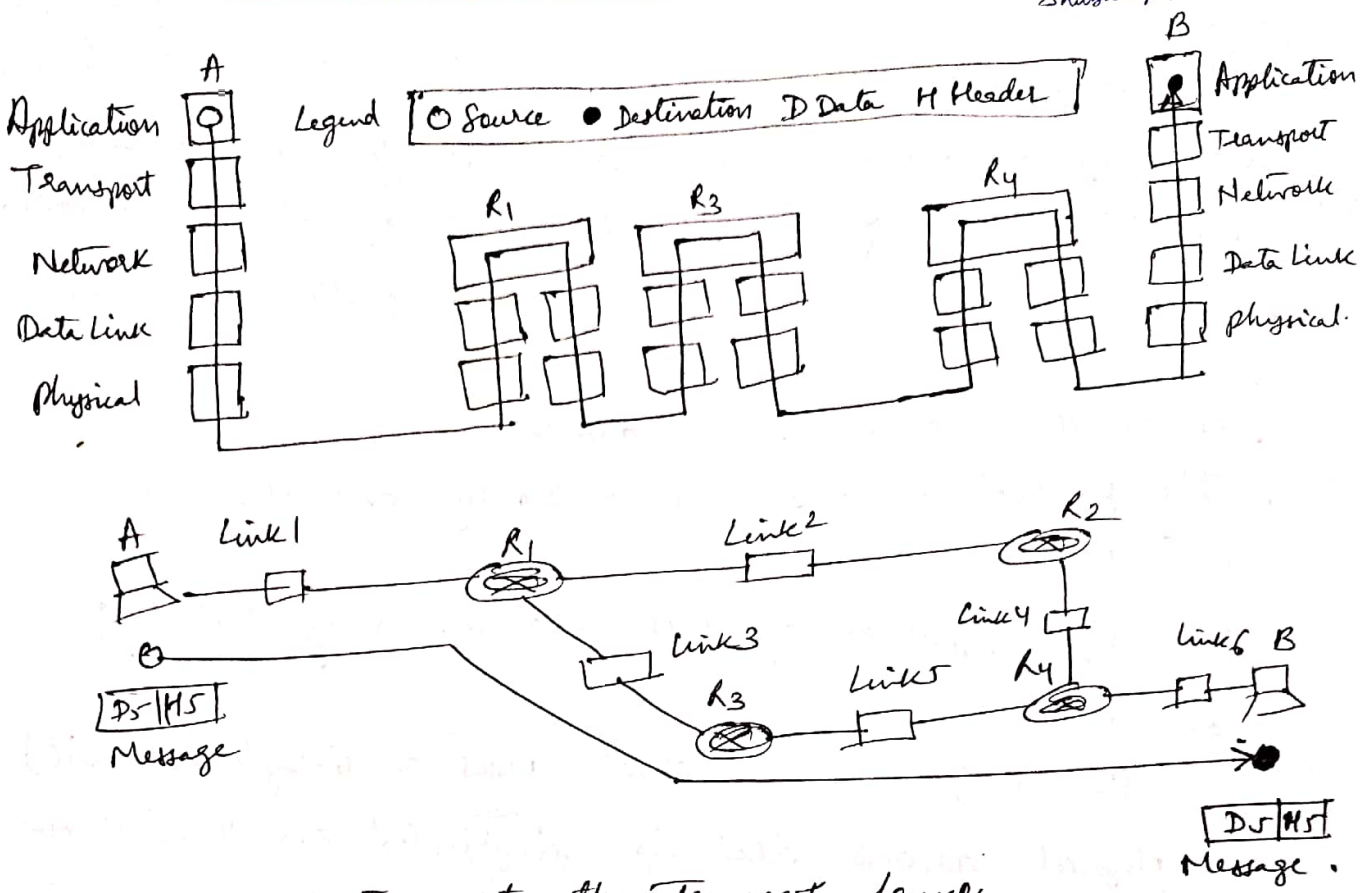
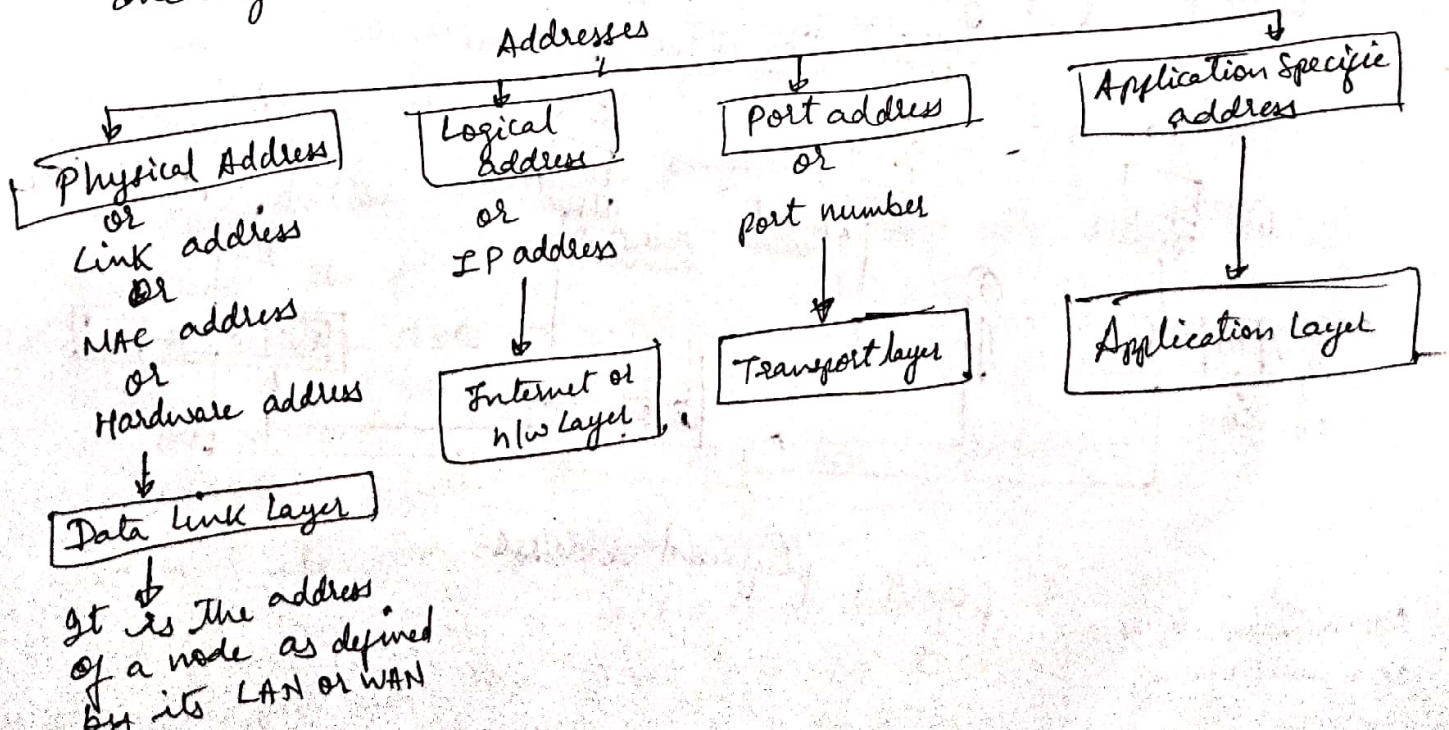


fig8: Communication at the Transport layer.

ADDRESSING:

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical address, logical address, port address & application-specific address. Each address is related to a one layer in the TCP/IP architecture.



Physical Addresses

- The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN.
- It is included in the frame used by the data link layer.
- It is the lowest-level address.
- The physical addresses have authority over the link (LAN or WAN).
- The size & format of these addresses vary depending on the n/w.
- for e.g., the Ethernet uses a 6-byte (48 bit) physical address that is imprinted on the network interface card (NIC). So LocalTalk (Apple), however, has a 1-byte dynamic address that changes each time the station comes up.

Example of physical addresses

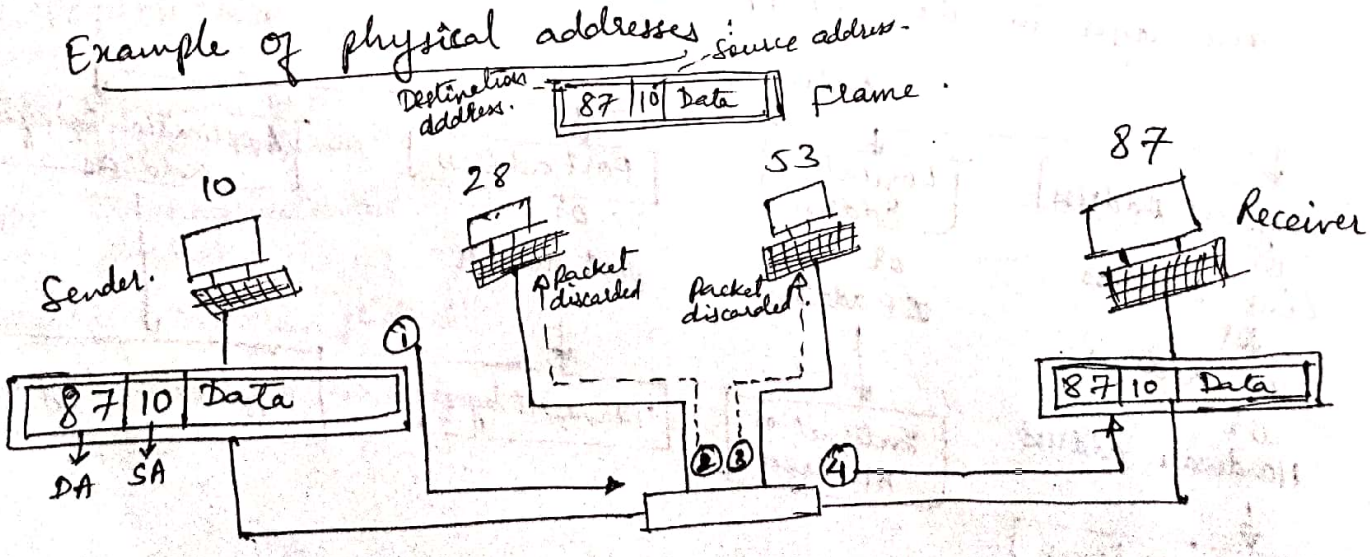


fig 9: physical addresses

DA → Destination address
SA → Source Address.

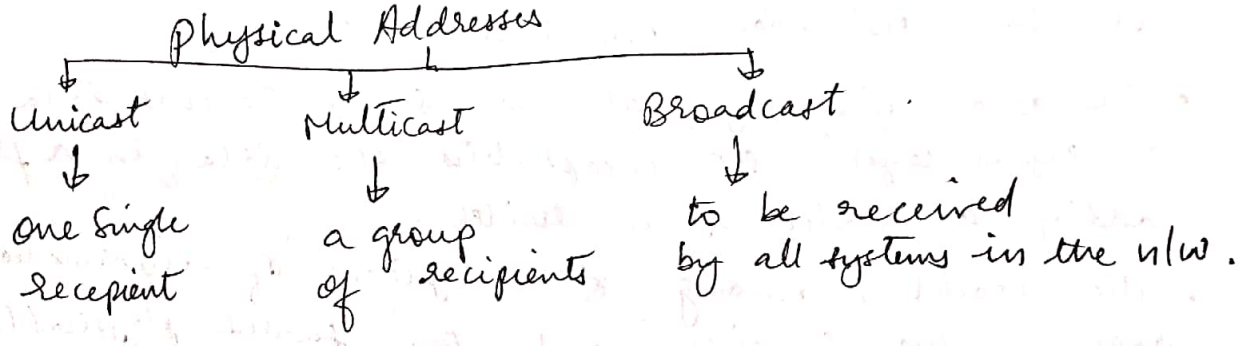
- In above figure, a node with physical address 10 sends a frame to a node with physical address 87.
- The two nodes are connected by a link (a LAN).
- At the data link layer, this frame contains physical (link) addresses in the header. These are the only addresses needed. The rest of the header contains other information needed at this level.
- The trailer usually contains extra bits needed for error detection.
- As in figure, the computer with physical address 10 is the sender, and the computer with physical address 87 is the destination (or receiver).
- The data link layer at the sender receives data from an upper layer. It encapsulates the data in a frame, adding a header & a trailer.
- The header, among other pieces of information, carries the receiver and the sender physical (link) addresses.
- Note that in most data link protocols, the destination address 87 in this case, comes before the source address (10 in this case).
- The frame is propagated through the LAN.
- Each station with a physical address other than 87 drops the frame because the destination address in the frame does not match its own physical address.
- The intended destination computer, however, finds a match between the destination address in the frame and its own physical address.
- The frame is checked, the header & trailer are dropped, & the data part is decapsulated & delivered to the upper layer.

Example of Physical Address (or Link Address or MAC address or Hardware address)

- Most local area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits, every byte (2 hexadecimal digits) is separated by a colon.

e.g. 07:01:02:01:2c:4B

A 6-byte (12-hexadecimal digits) physical Address.



for e.g. Ethernet supports the unicast physical addresses (6 bytes), the multicast addresses & the broadcast addresses.

- Some networks do not support the multicast or broadcast physical addresses.

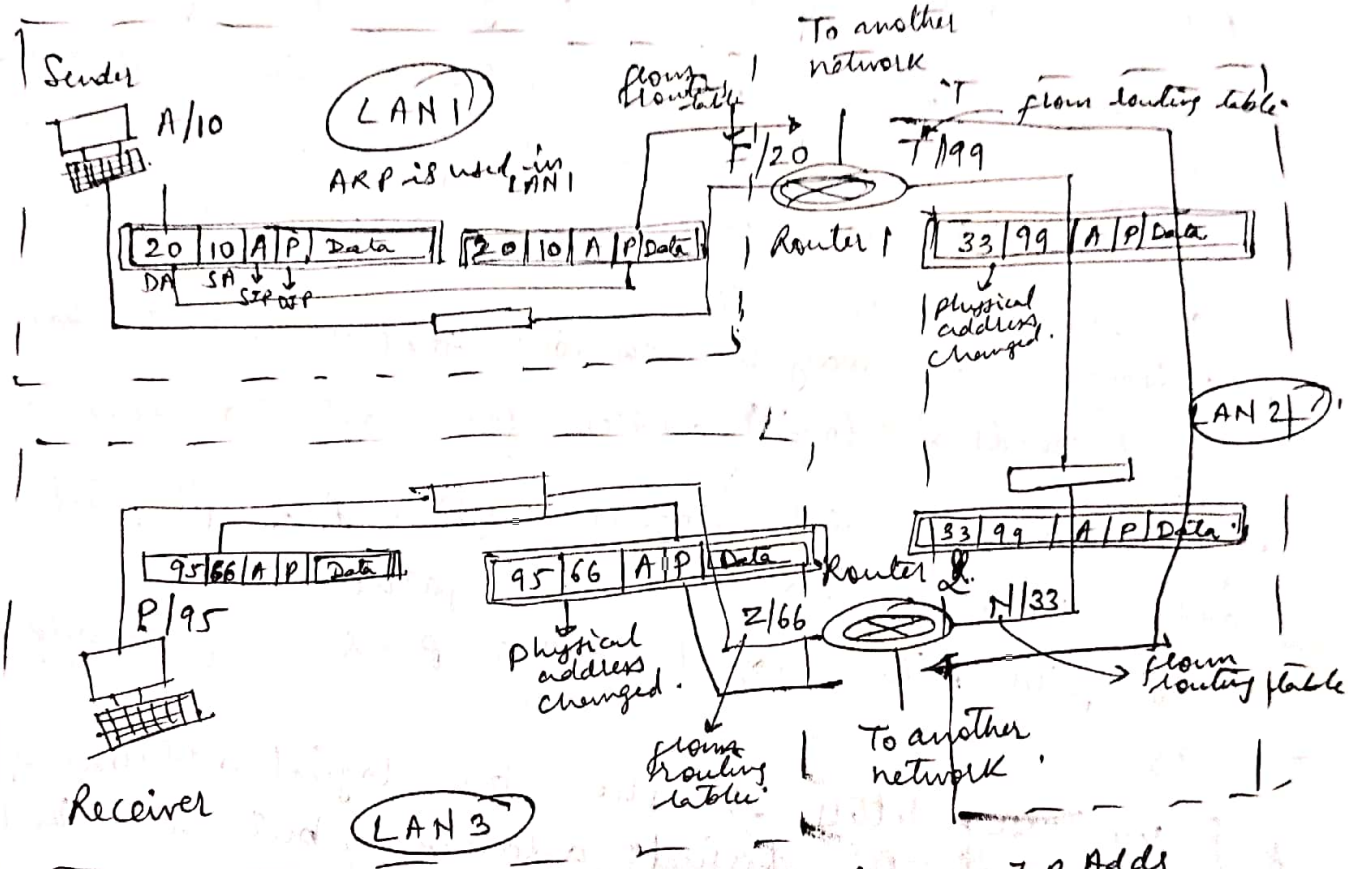
Logical Addresses

- Logical addresses are necessary for universal communications that are independent of underlying physical networks.

*. Physical addresses are not adequate in an internetwork environment where different networks can have different address formats.

- A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network.

- The logical addresses are designed for this purpose.
- A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet.
- No two publicly addressed and visible hosts on the Internet can have the same IP address.



SIP → Source IP Addr
DIP → Destination IP Addr.
DA → Destination MAC Addr (Physical)
SA → Source MAC Addr (Physical)

fig 10: Logical Addresses

★ Physical addresses will change from hop to hop, but the logical addresses remain the same.

Logical addres can be

- Unicast
- Multicast
- Broadcast.
  - There are limitations on broadcast addresses.

Fig 10 shows a part of an internet with two routers connecting three LANs.

- Each device (computer or router) has a pair of addresses (logical & physical) for each connection.
- In this case, each computer is connected to only one link and therefore has only one pair of addresses.
- Each router, however, is connected to three networks (only two are shown in the figure).
- So each router has three pairs of addresses, one for each connection.
- Although it may be obvious ~~that each router has~~ why it needs a logical address for each connection.
- The computer with logical address A & physical address 10 needs to send a packet to the computer with logical address P & physical address 95.

* [We use letters to show the logical addresses & numbers for physical addresses, but note that both are actually numbers.
e.g. logical address A can be 168.3.2.1
& physical address 10 can be 48:12:F1:AB:33:CD]

- The Sender encapsulates its data in a packet at the n/w layer & adds two logical addresses (A & P)
- Note that in most protocols, the logical source address comes before the logical destination address (contrary to the order of physical addresses).

i.e.

Destination MAC Addr	Source MAC Addr	Source IP Addr	Destination IP Addr

- The network layer, however, needs to find the physical address of the next hop before the packet can be delivered.
- The n/w layer consults its routing table & finds the logical address of the next hop (router 1) to be F
- Another protocol, Address Resolution Protocol (ARP), finds the physical address of router 1 that corresponds to its logical address (20).
- Now the n/w layer passes this address to the data link layer, which in turn encapsulates the packet with physical destination address 20 & physical source address 10.
- The frame is received by every device on LAN 1, but is discarded by all except router 1, which finds that the destination physical address in the frame matches with its own physical address.
- The router decapsulates the packet from the frame to read the logical destination address P. Since the logical destination address does not match the router's logical address, the router knows that the packet needs to be forwarded. The router consults its routing table & ARP to find the physical destination address of the next hop (router 2), creates a new frame, encapsulates the packet & sends it to the router 2.
- Note the physical addresses in the frame. The source physical addresses changes from 10 to 99. The destination physical address changes from 20 (router 1 physical address) to 33 (router 2 physical addr)

- The logical source & destination addresses must remain the same; otherwise the packet will be lost.
- At router 2 we have a similar scenario. The physical addresses are changed, & a new frame is sent to the destination computer. When the frame reaches the destination, the packet is decapsulated. The destination logical address matches the logical address of the computer. The data are decapsulated from the packet & delivered to the upper layer.

* Note that although the physical addresses will change from hop to hop, logical addresses remain the same from source to destination.

Port Addresses

- The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host.
- However, arrival at the destination host is not the final objective of data communications on the Internet.
- A system that sends nothing but data from one computer to another is not complete.
- Today, computers are devices that can run multiple processes at the same time.
- The objective of Internet communication is a process communicating with another process.

Shubhangi K

- For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the file transfer protocol (FTP).
- For these processes to receive data simultaneously, we need a method ~~to~~ label the different processes. In other words, they need addresses.

In the TCP/IP architecture, the label assignment to a process is called a port address. A port address in TCP/IP is 16 bits in length.

Example of port numbers:

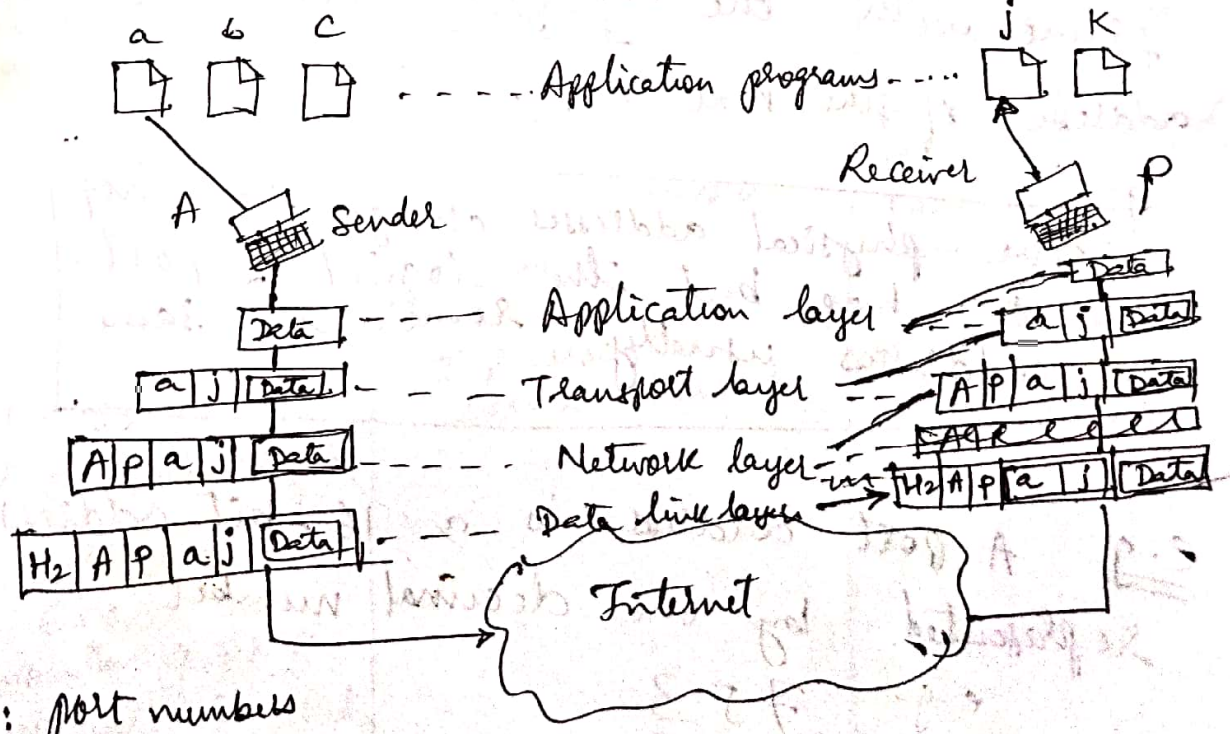


fig 11: port numbers

fig 11 shows two computers communicating via the Internet.

- The sending computer is running three processes at this time with port addresses a, b & c
- The receiving computer is running two processes at this time with port addresses j & k.
- Process a in the sending computer needs to communicate with process j in the receiving computer.

- Note that although both computers are using same application, FTP, for example, the port addresses are different because one is a client program & the other is the server program (e.g. FTP port 20 & 21)
- To show that data from process a need to be delivered to process j, & not k, the transport layer encapsulates data from the application layer in a packet & adds two port addresses. (a & j), source & distination. The packet from the transport layer is then encapsulated in another packet at the nlw layer with logical source & distination addresses (A & B). Finally, this packet is encapsulated in a frame with the physical source & destination addresses of the next hop.

> The physical addresses change from hop to hop, but the logical & port addresses usually remain the same

e-g A port address is a 16-bit address represented by one decimal number
e.g. 753

Application - Specific Addresses

- Some applications have user-friendly addresses that are designed for that specific application -
- Examples include the e-mail address (for eg. forouzan@fida.edu) & Universal Resource Locator (URL) (for example, www.mhhe.com).

Shubhangi K

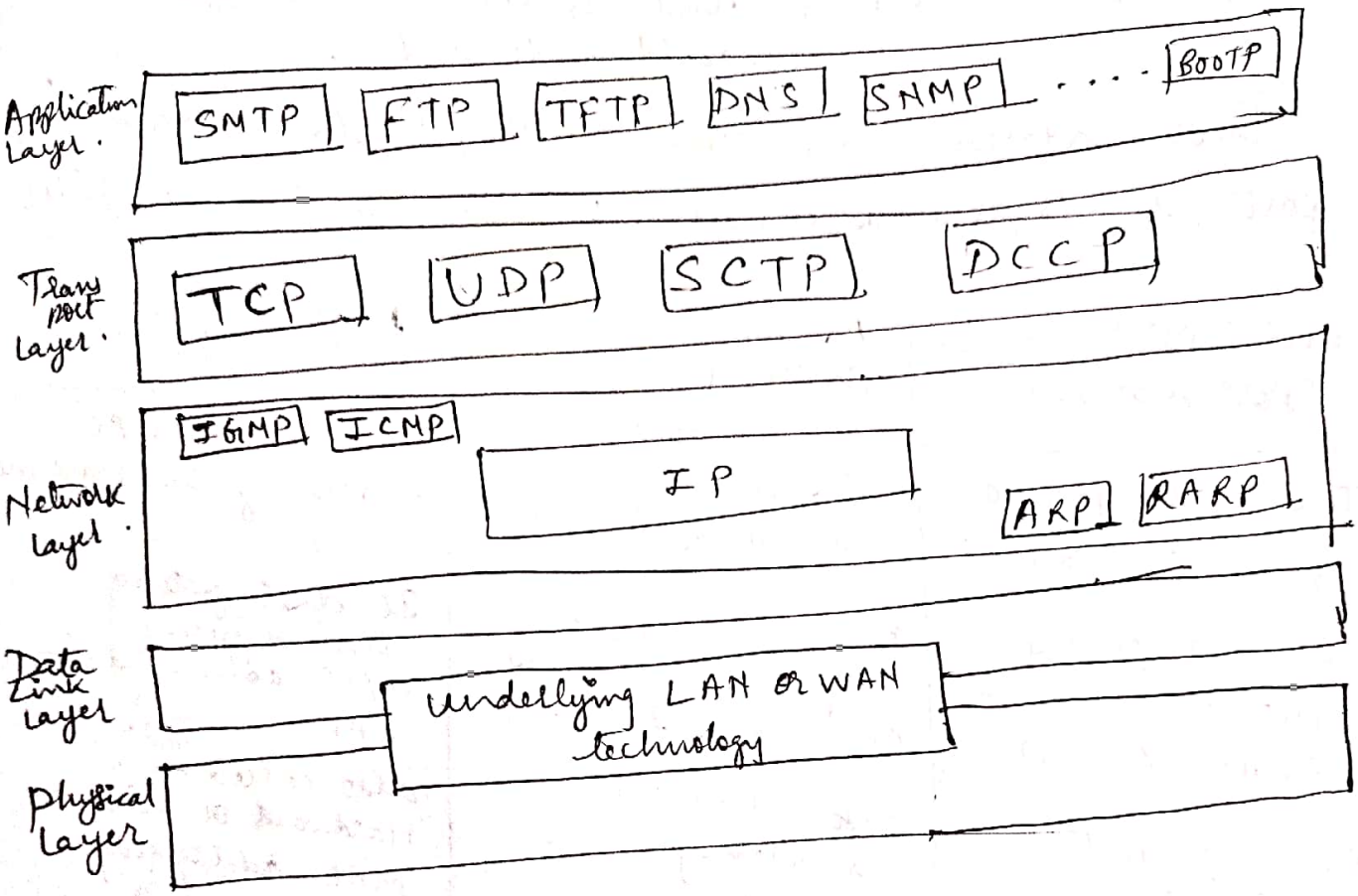
forouzan @ fhda.edu ⇒ recipient of an email

www.mhhe.com ⇒ used to find a document on the world wide web.

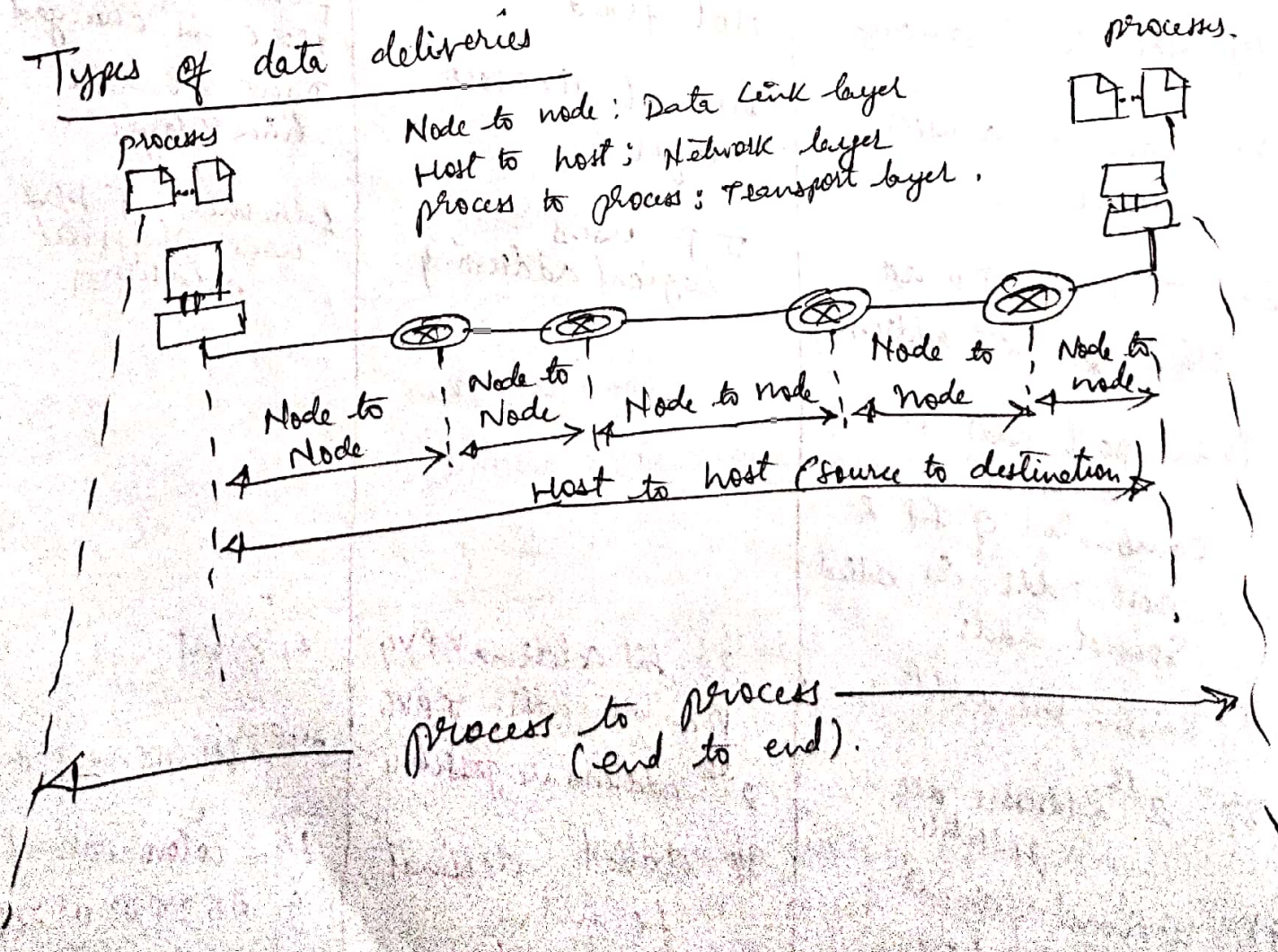
These addresses are then changed to corresponding port & logical addresses by the sending computer.

Service Point Addressing (Port Addresses)	Logical Addressing	Physical Addressing
1) This is the port no of the application	This is the IP address of the machine	This is the MAC address of the machine.
2) It distinguishes applications on the m/c's (eg HTTP & SMTP)	It distinguishes two different machines connected in Internet	It distinguishes two different m/c's connected in LAN
3) Also called port addressing	also called IP addressing	also called Hardware or Link or MAC addressing.
4) Not fixed always	Not fixed	fixed unless NIC is changed.
5) Done at transport layer	Done at Network layer	Done at data link layer.
6) TCP & UDP ~~used~~ port addressing	IP uses logical addressing	Ethernet, FDDI uses physical addressing.
Max port addr is 65535		
Combination of IP & port addr is called Socket addr.		
7) 16-bit addr.	32-bit addr → IPV4	48 bit
8) 2^{16} addresses are possible	128-bit addr - IPV6	2^{48} addresses are possible.
9) decimal format e.g. 753	2^{32} addresses are possible	Hex colon format e.g. AB:CD:11:22:FE:56
	9) dotted decimal format e.g. 192.3.2.1/24	

Layerwise protocols in TCP/IP Architecture



Types of data deliveries



Shubhangi K

Node-to-Node delivery: The data link layer is responsible for delivery of frames between two neighboring nodes over a link. This is called node-to-node delivery.

Host to Host delivery: The n/w layer is responsible for delivery of datagrams between two hosts. This is called host to host delivery.

process-to-process delivery: The transport layer is responsible for process to process delivery — the delivery of a packet, part of a message, from one process to another.

- Two processes communicate in a client/server relationship.

Client/Server Paradigm:

Client/Server paradigm is one of the several ways to achieve process-to-process communication.

- **client**: It is the process on a local host,
- **server**: It is the process on a remote host.

Both processes (client & server) have the same name.

For e.g., to get the day & time from a remote machine, we need a Daytime client process running on the local host & a Daytime server process running on a remote machine.

e.g. Wednesday 9:00am

Operating systems today support both multiuser & multiprogramming environments. A remote computer can run several server programs at the same time, just as the local computers can run one or more client programs at the same time.

For communication, we must define the following:

1. local host
2. local process
3. remote host
4. remote process.

Addressing:

Whenever we need to deliver something to one specific destination among many, we need an address.

At data link layer, we need a MAC address to choose one node among several nodes if the connection is not point to point.

- A frame in the data link layer needs a destination MAC address for delivery and a source address for the next nodes reply.

At the network layer, we need an IP address to choose one host among millions.

- A datagram in the network layer needs a destination IP address for delivery and a source IP address for the destination's reply.

At the transport layer, we need a transport layer address, called a port number, to choose among multiple processes running on the destination host.

- The destination port no is needed for the delivery; the source port no is needed for the reply.

In the Internet model (TCP/IP model), the port numbers are 16-bit integers between 0 and 65535. The client program defines itself with a port number, chosen randomly by the transport layer software running on the client host. This is the ephemeral port number.

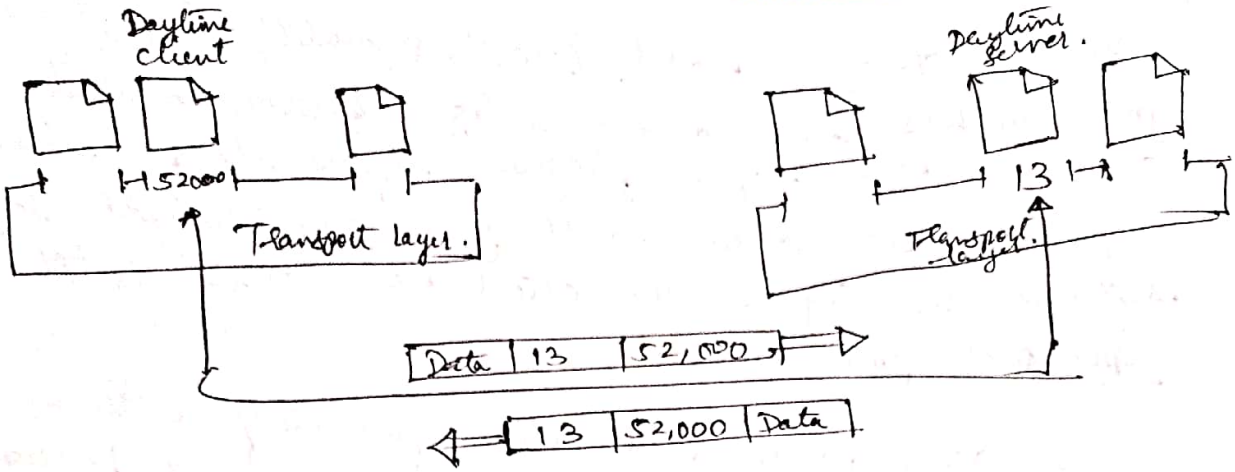
The server process must also define itself with a port number. This port number, however, cannot be chosen randomly. If the computer at the server site runs a server process & assigns a random number as the port number, the process at the client site that wants to access that server and use its services will not know the port number. Of course, one solution would be to send a special packet & request the port number of a specific server, but this requires more overhead.

The Internet has decided to use universal port numbers for servers; these are called well-known port numbers. There are some exceptions to this rule; for example, there are clients that are assigned well-known port numbers. Every client process knows the well-known port number of the server process.

For example, while the Daytime client process, can use an ephemeral (temporary) port number 52000 to identify itself, the Daytime server process must use the well-known (permanent) port number 13.

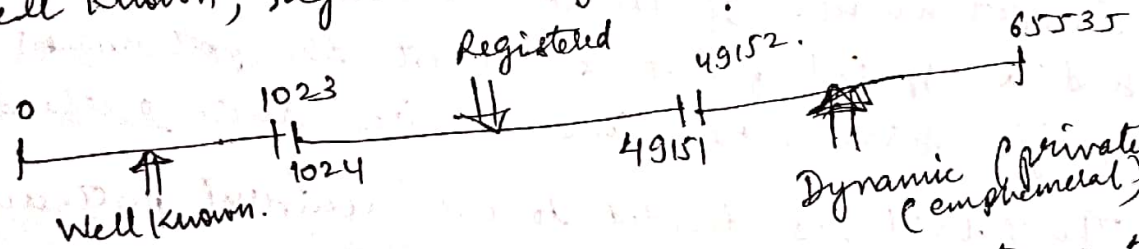
Ephemeral → Temporary

Well-Known → Permanent



IANA Ranges

The IANA (Internet Assigned Number Authority) has devided the port numbers into three ranges:
Well Known, registered & dynamic (private)



- **Well-Known ports**: The ports ranging from 0 to 1023 are assigned & controlled by IANA. These are the well-known ports.
- **Registered ports**: The ports ranging from 1024 to 49151 are not assigned or controlled by IANA. They can only be registered with IANA to prevent duplication.
- **Dynamic ports**: The ports ranging from 49,152 to 65535 are neither controlled nor registered. They can be used by any process. These are the Emphemeral ports

Ephemeral ports = Lasting for very short time

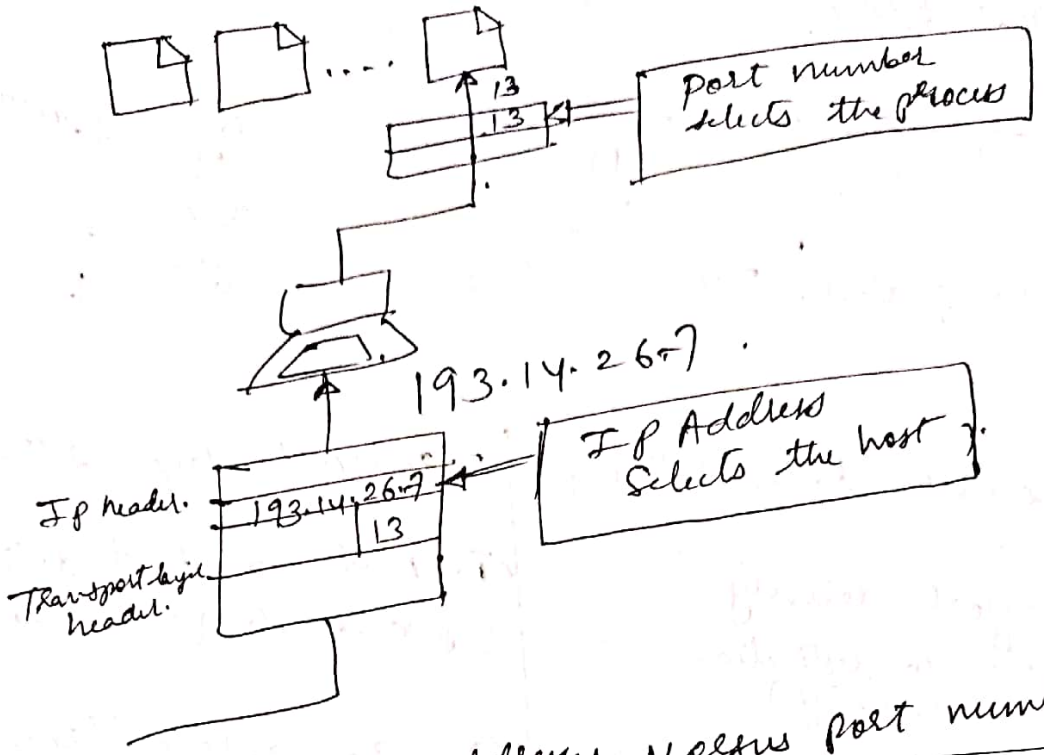


fig: IP addresses versus port numbers.

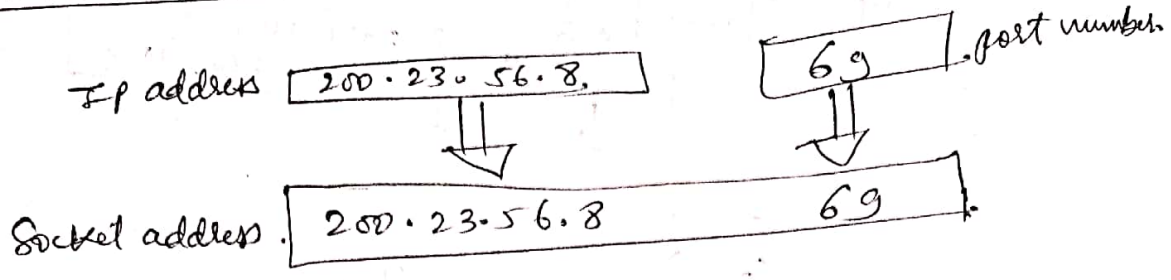
Socket Addresses.

Process-to-process delivery needs two identifiers, IP address & the port number, at each end to make a connection. The combination of an IP address & a port number is called a socket address. The client socket address defines the client process uniquely just as the server socket address defines the server process uniquely.

A transport layer protocol needs a pair of socket addresses: the client socket address and the server socket address. These four pieces of information are part of the IP header and the transport layer protocol header. The IP header contains the IP addresses; the TCP or UDP header contains the port numbers.

Shubhangi K

fig: Socket Address



Network layer delivery	Transport layer delivery
① Best effort delivery (source to destination delivery)	① End to End delivery (process to process delivery)
② Does not guarantee transmission	② Gaurantee transmission
③ Not reliable, does not provide error & flow control	③ Reliable, provides error & flow control.
④ connectionless	④ connectionless or connection oriented.
⑤ packets or datagrams.	⑤ TCP segments UDP → datagrams SCTP → packets.
⑥ uses IP address	⑥ uses port address.

Data Link Layer delivery

1) Reliable
2) Frames are used for information transfer
3) Uses MAC address (phy) link (HW addr
   eg AB:C1:23:14:36:F2
4) Node to Node delivery (Hop-by-Hop)

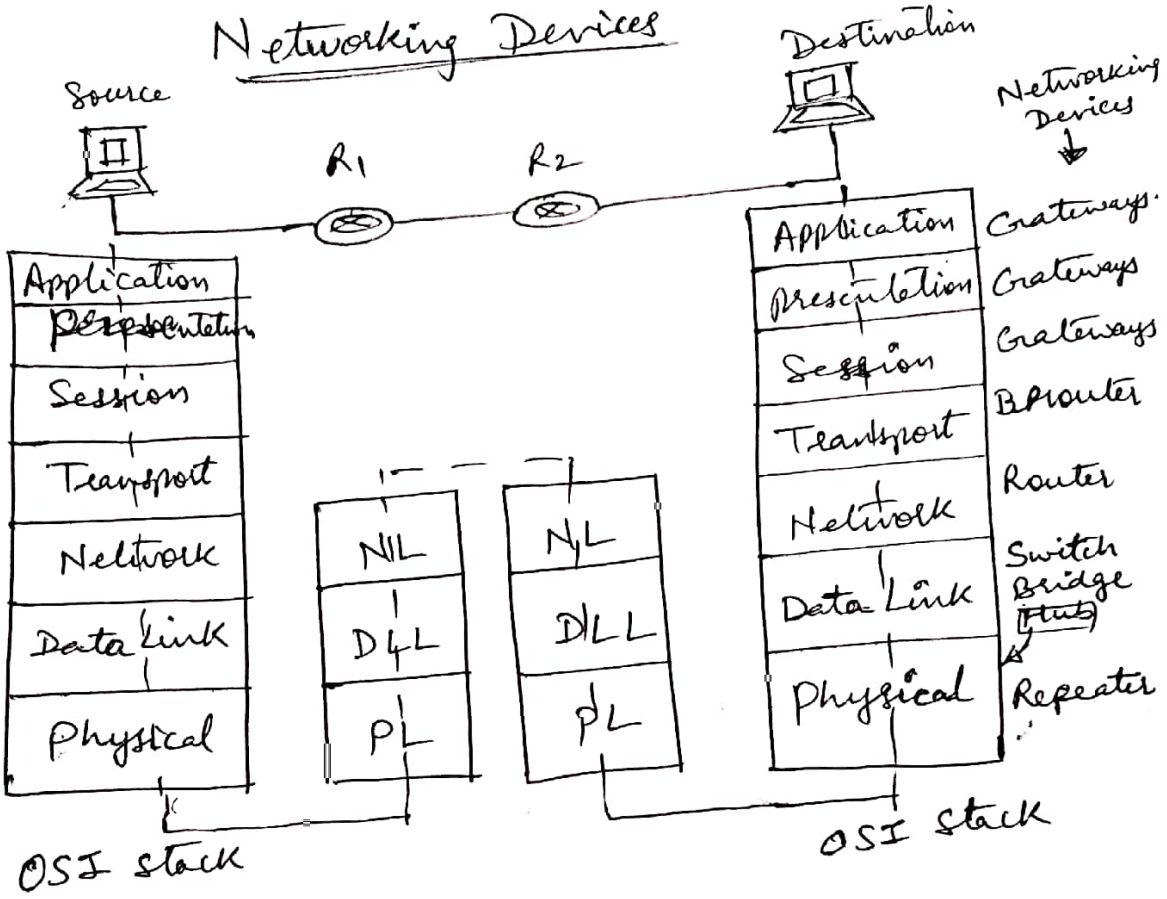
(Shubhangi K)

Comparison between OSI model & TCP/IP Architecture.

ISO OSI model	TCP/IP Architecture / Internet Model
(1) There are 7 layers	(1) There are 4 layers → in original Model Now there are 5 layers
(2) OSI is a model & not a protocol	(2) TCP/IP is a protocol not a model
(3) Was developed after TCP/IP	(3) was developed before OSI model
(4) In OSI model was devised first & then the protocols were invented.	(4) In TCP/IP the protocol was developed first & then the architecture was developed
(5) Clearly distinguishes between Service, interface & protocol	(5) Does not clearly distinguish between service, interface & protocols
(6) Do not support Internetworking	(6) Supports Internetworking
(7) Supports both connectionless & connection oriented Communication in network layer.	(7) Supports both Connectionless & connection oriented Communication in transport layer but supports only connectionless Communication in network layer
(8) OSI model is strictly layered	(8) TCP/IP Architecture is loosely layered
(9) Vertical Horizontal approach (Transport layer of source can directly talk to Trans layer of dest)	(9) ~~Horizontal Approach~~ Vertical Approach (each layer is transparent)

Shubhangi Khaire

Networking Devices



Shubhangi Khatke

HUB or Ethernet Hub

- Hub is a network device
- It connects multiple Ethernet devices together
- A hub works at the physical layer (layer 1) of the OSI Model.
- The device is a form of multiport repeater (Every port of a hub repeats or reconstructs the received signal & then broadcasts it)
- Types of Hubs:
  - **Active Hubs**: Reconstruct or repeat (regenerate) the received signals. Needs power for its operation
  - **Passive Hubs**: Do not reconstruct or repeat the received signals. Do not need power for its operation
  - **Intelligent / Smart Hubs**:
    - Enables an administrator to monitor the traffic passing through the Hub
    - Enables an administrator to configure each port in the Hub.
    - Intelligent Hubs are also called Manageable hubs.

Shubhangi Khalche

24 port Hubb

- Hub receives information on a port & broadcasts it to all other ports.
- Since broadcasting is done, all devices receive the information but only the intended receiver receives it whereas all other devices discard the information.
- Since every time Hub broadcasts the information, a lot of traffic is generated in the network.
- Thus problem of congestion arises while communication is done with a Hub.
- The signals from all devices collide in a single collision domain.
- Hub does not understand any kind of address.

* Difference Between Hub & a Switch

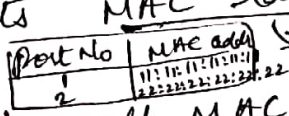
(Shubhangi Khatke)

	Hub	Switch
Layer in OSI Model	Physical layer (Layer 1 Device)	Data Link Layer (Layer 2 Devices)
Transmission Type	Only Broadcast	At Initial level Broadcast then Unicast & Multicast
Table	There is no MAC Table in Hub, Hub can't learn MAC address	Store MAC address in lookup table, Switch can Learn MAC address
Usage	LAN	LAN
Ports	4 Ports	24/48 Ports
Collision	In Hub Collision occurs	In Full duplex Mode no Collision occurs
Transmission Mode	Half Duplex	Full duplex
collision domain	Hub has one collision domain	In switch, every port has its own collision domain
cost	Cheaper than Switches	3-4 Times costlier than Hub
Broadcast Domain	Hub has one Broadcast Domain	Switch has one Broadcast Domain

Shubhangi Kharche

Switch

- It is Layer 2 Device (used at Layer 2 of OSI model)
- It has number of ports (usually even) to connect devices in a LAN.
- It connects devices (computers, printers, laptops) in a LAN
- Switch initially broadcasts the information received on a port.
- Gradually learns all MAC addresses, understands which PC is connected to which port number & the MAC address.
- Switch Maintains the port number & MAC address entries in its MAC table (ARP table) or (forwarding table)



- Later on after learning all MAC addresses, it may simply unicast or multicast the received information.
- Since switch follows unicasting & uses full-duplex transmission, the devices connected to a switch forms different collision domains.
- Switch connects devices belonging to a single LAN technology i.e. either Ethernet or Token ring but not both. (or switch can connect devices belonging to FDDI technology only, or Ethernet only, or Token ring only or Token bus only or ATM only but does not connect devices belonging to diff technologies or protocols).

- Switch is an intelligent device, it understands MAC address.
- It receives frames on a port, makes a lookup in its MAC table for the destination MAC address & forwards the frame to that MAC address only using unicast address
- Some switches operate at n/w layer (L-3)
- If a Sw operates at L-2 & L-3, it is called as multilayer Switch.
- Switch generates separate collision domains (Each port of a switch operates in a separate collision domain)
- Switch provides high speed data exchange @ 10MBPS, @ 100MBPS, @ 1000MBPS @ 10GBPS.
- Low Latency.
- Dedicated comm bet^n devices (unicast, point to point).

★ Difference Between Switch & Router (networking Devices)

Switch	Router
1) It is the LAN device	1) It is the WAN device
2) Switch maintains MAC tables	2) Router maintains IP tables (routing) tables
3) Switch understands MAC address (Hardware/ Physical / Link) address	3) Router understands IP address (logical address)
4) Switch connects devices in a LAN or Switch connects devices belonging to two similar LAN's together	4) Router connects more than two dissimilar networks together. Router connects LAN to a WAN. Router can connect Ethernet LAN with token ring LAN (dissimilar n/w's)
5) Switch is an Intranetworking device (LAN)	5) Router is an Internetworking device (Connects diff n/w's in WAN or Internet)
6) Switch is Layer 2 networking device (used at Layer 2 of OSI model)	6) Router is Layer 3 networking device (used at Layer 3 of OSI model)
7) In Full Duplex Switch no collision occurs	7) No collisions
8) Full Duplex Transmission	8) Full Duplex Transmission
~~9) Speed : 1-10 Mbps (Video) 100 Mbps (max)~~	~~Speed 10/100 Mbps~~ 1 Gbps

Shubhangi Khalche

	Switch	Router
9)	Speed → 10/100 MbPS, 1 GbPS	Speed 1-10 MbPS (wireless), 100 MbPS (wired)
10)	Switch has one Broadcast domain	Every port has its own Broadcast domain
11)	Takes more Time for complicated Switching decision	Takes faster routing decision

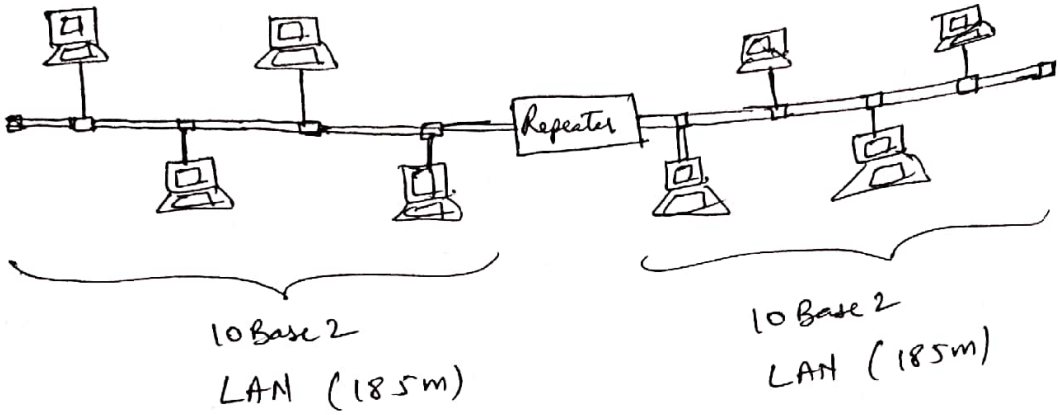
(Shubhangi Khalkhe)

Repeater

- A repeater is an electronic device that receives a signal and retransmits it at a higher level and/or higher power.
- Repeater is a networking device
- used to regenerate or replicate a signal
- Regenerate analog or digital signals distorted by transmission loss.
- Works at Layer 1 of OSI model (at physical layer)
- Repeater removes the impurities from the received signal, reconstructs it & then transmits it whereas an amplifier amplifies the received signal with impurities.
- Repeater receives data in the form of bits (0's & 1's), reconstructs it & then transmits the data.
- Repeaters can be classified as analog or digital repeaters.
- Analog repeaters only amplify the signal (do not remove impurities)
- Digital repeaters can reconstruct (removes impurities) a signal to its original Quality.

Shubhangi Khalche

Repeaters (contd...)

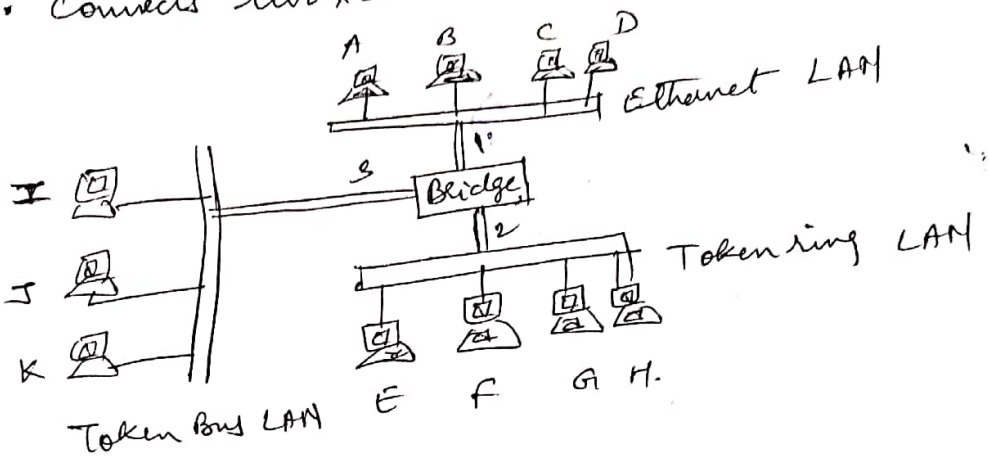


- If we want to connect two 10 Base 2 LAN together then repeater is required to signal reconstruction.

Network Bridge

Shubhangi Khaleke

- Layer 2 (Data Link layer) device (OSI Model)
- Connects two or more dissimilar LAN's together.



- Has 2 to 3 ports
- Has 2 to 3 Network Interface cards. (each for one LAN)
- Maintains MAC Tables.

Port No	MAC Address
1	M_A, M_B, M_C, M_D
2	M_E, M_F, M_G, M_H
3	M_I, M_J, M_K

$M_A \Rightarrow$ MAC Address of m/c A

$M_B \Rightarrow$ MAC Address of m/c B

& so on.

- Bridge filters frames
- Bridge minimises congestion by dividing LAN segments.
- Has memory to store MAC Tables.
- Has processing capability (More 'intelligent' than Switch)

	Repeater	Hub	Switch	Bridge	Router
1)	Layer 1 (Phy) of OSI Model	Layer 1 (Physical) of OSI Model	Layer 2 (~~Phy~~) Data Link of OSI Model	Layer 2 (Data Link) of OSI Model	Layer 3 (Network Layer of OSI Model)
2)	Regenerates the Signal (extends LAN Segments)	connects computers ~~together~~ (Multiport repeater as it regenerates the signal)	connects computers in LAN or connects two Similar LAN Segments together (Ethernet to Ethernet) or (Token-ring to Token-ring) → 10Base2 to 10Base F or 10Base T to 10Base F	connects two dissimilar LAN's together (Ethernet to Token ring) or (Ethernet to FDDI)	connects two dissimilar n/w's together (LAN to WAN) (Ethernet & FDDI LANs to WAN)
3)	Does not have filtering capability	Does not have filtering capability	~~Does not Has~~ filtering capability	filters frames (Has filtering capability)	filters packets
4)	Dumb device	Dumb device	Intelligent device	More Intelligent than Switch	Intelligent device

	Repeater	Hub	Switch	Bridge	Router
(5)	It has Two ports	usually has 4 ports 5th port connects to another Hub (Hubs generally have even no of ports 4, 8, 12, 16, 24 Maximum 24 ports	usually has even number of ports	less no of ports than Switch (2-3 ports)	Minimum two Interfaces (Maximum can be upto 100) Routers have Five ports 1) console port (connects to PC) 2) auxiliary port (connects to internet) 3) LAN port (RJ-45) (connects to Ethernet, Fast Ethernet or Gigabit Ethernet) 4) WAN Port (Serial Interface, RJ-11 ⇒ Telephone line) (Serial connects → Router to Router) 5) USB Port.
(6)	No Memory	No Memory	Memory to save MAC tables	Memory to save MAC tables Also has processing capability	Memory → RAM • Running OS • Running configuration file • IP routing tables, ARP tables • Packet buffer. ROM • permanent OS • Bootstrapping Flash • IOS • other system files NV-RAM • start-up configuration

Shubham Khanna

Shubhangi Khaiche

Repeater	Hub	Switch	Bridge	Router
(7)	• Single collision domain • All ports (all m/c's) lie in single collision domain • Information is always Broadcasted	Separate collision domains (NO collisions) (Each port of a switch lies in separate collision domain • Broadcasting when S/w is initialised later on Unicasting or Multicasting.	• Separate Broadcasting & collision domains	• Removes congestion • Does Traffic Management.

Shubhangi Khaiche.

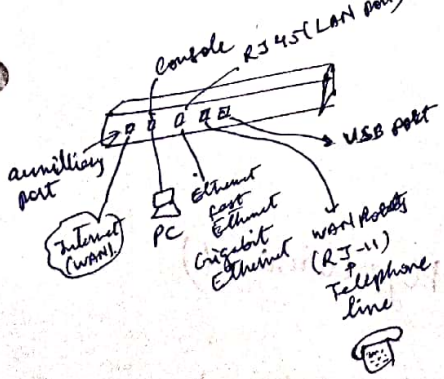
Shubhangi Khaeche

What is a Router ?

- Router is Interconnecting device (Internetworking device)
- Router is an Intelligent Device
- Router acts as a Gateway
- Router is layer 3 device (Network Layer)
- Router understands IP address.
- Router has operating system (Example- IOS, SunOS, NOS, Comvale)
- Router has routing features & tons of other features.
- Router controls traffic automatically, performs load balancing automatically.
- Router has minimum two interfaces.

Router manufacturers (Cisco, D-Link, TP Link, BSNL, Netgear, Juniper etc).

- Router port → auxilliary ↔ To connect with internet (remote).
  - → console (Local port)
    - ↳ To connect PC
  - → LAN port (RJ-45) → Ethernet, Fast ethernet, Gigabit Ethernet
  - → WAN ports (Serial ports, RJ 11) ↳ phone line
  - → USB port

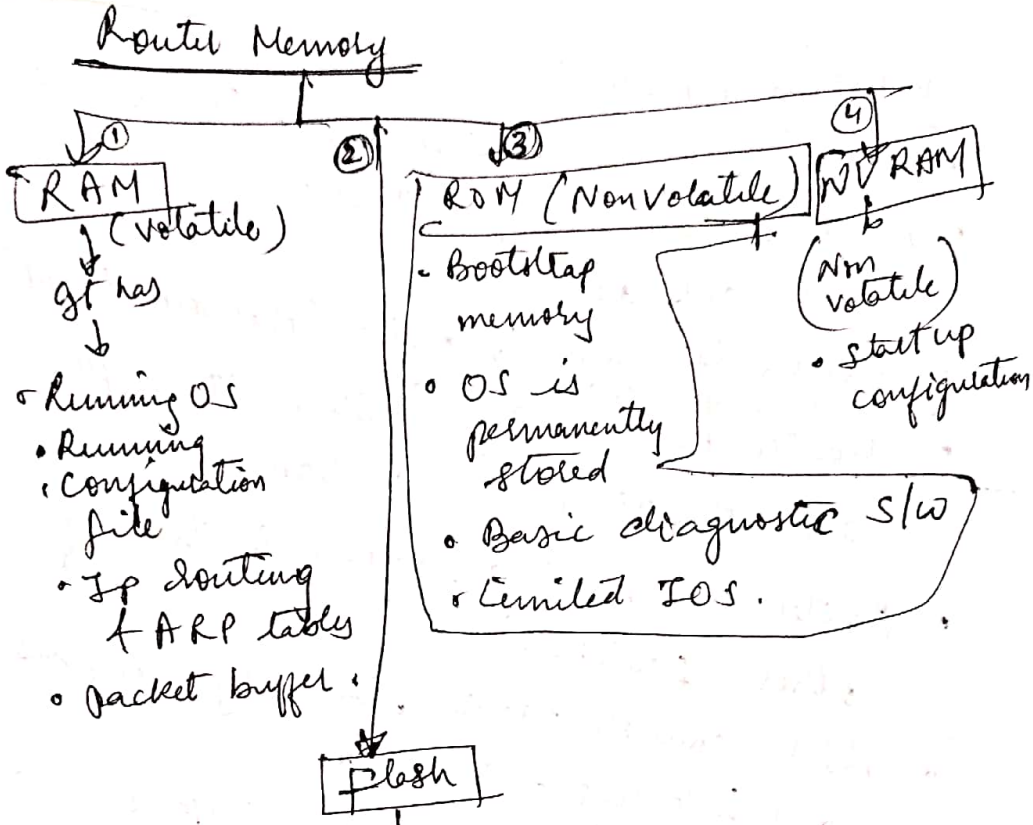


For External use
↓
auxilliary, LAN port, WAN ports, USB port.

Computer	Router
1) Has Processor	• Has processor
System 2) Has RAM, ROM	• Has RAM, ROM
Buses-3) Has I/O Buses	• Has IP Buses (System Buses)
4) Has monitor Keyboard, mouse	* Does not have monitor, Keyboard, mouse

Shubhangi Khalche

Router Memory



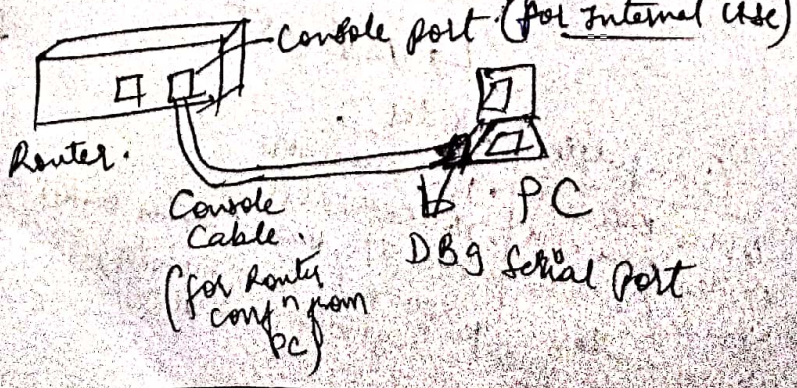
How to Use Router?

Two ways to Operate router

1) CLI
2) GUI

Accessing Tools

1) Simulator (Putty, SecureCrt, Hyperterminal)
2) Web Browser.



Shubhangi Kherche

- Router has Minimum two interfaces (May have 100 interfaces also)
- Router connects two dissimilar n/w's together (LAN to a WAN)
- Router forwards packets. Each packet header has source IP address & destination IP address.
- Router controls collision domains (can detect the collision domains)
- Router controls Broadcast domains (Router may or may not do Broadcasting depending on the requirements)
- Router acts as a Gateway.
- Router filters packets based on IP address
- Router maintains routing tables to take forwarding & routing decisions.

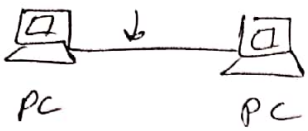
Shubhangi Kharche.

Gateway :

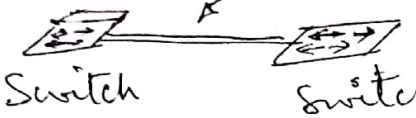
- Gateway is more intelligent device than a router
- It has the combination of both hardware & software
- operates on all layers above network layer.

Shubhangi Khalche

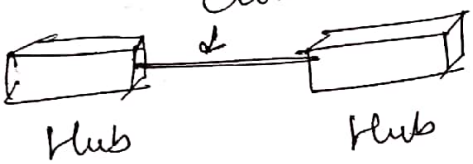
(UTP)
Crossover cable

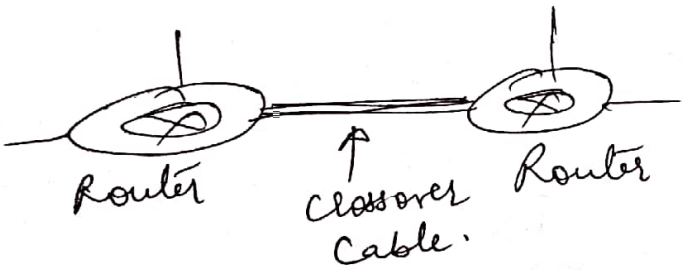


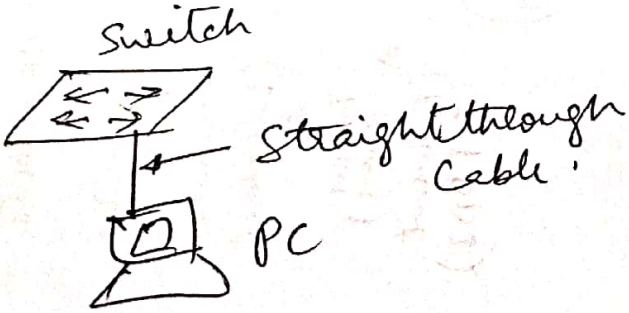
Crossover cable.



Crossover cable.





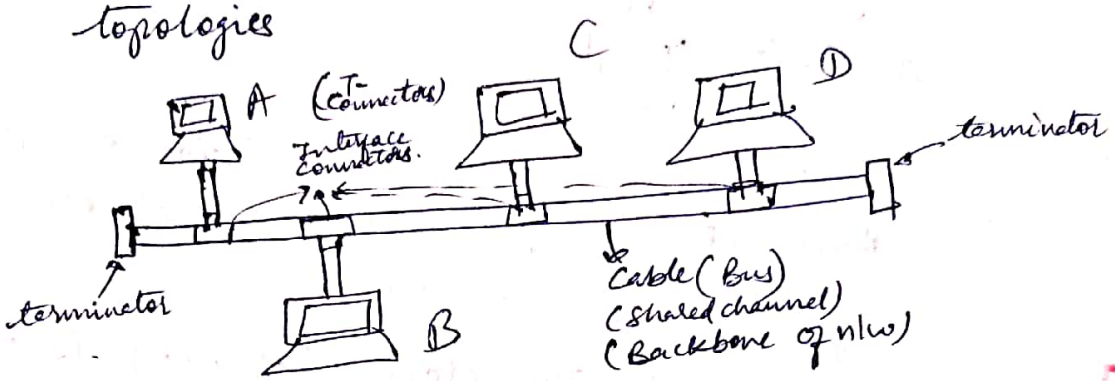


Shubhangi K

Network Topologies (Topology ⇒ Layout The way the devices are connected in a n/w)

① Bus Topology

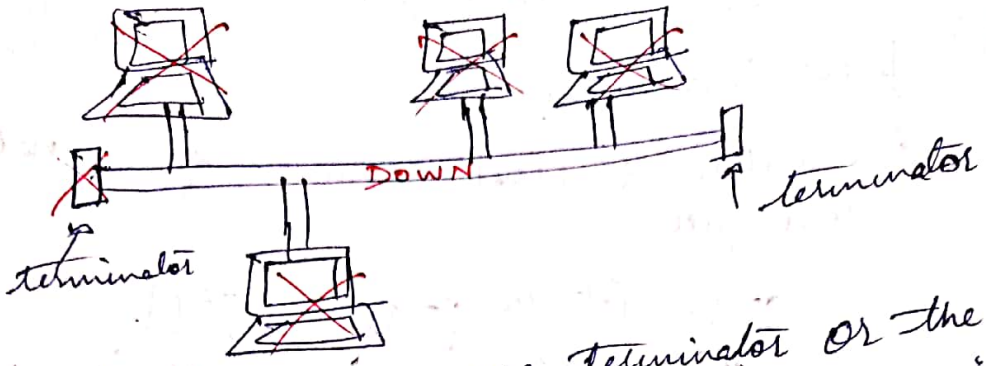
- Simplest & most common of all network topologies



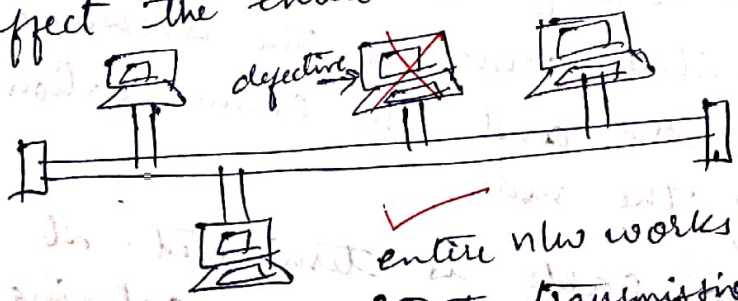
- computers or servers are connected to a single cable.
- Central cable is the backbone of the network and the communication means of the nodes.
- The cable is terminated at both the ends to prevent the echoing back of signals in the data transmission.
- Data transmission:

When m/c A wants to transmit data to m/c D, the signal transmitted from A is broadcast; it travels thro' the intermediate m/c's B & C but finally received by m/c D. The signal does not stop there, it moves towards the cable end where it is absorbed completely & does not travel back across the bus.

Shubhangi K

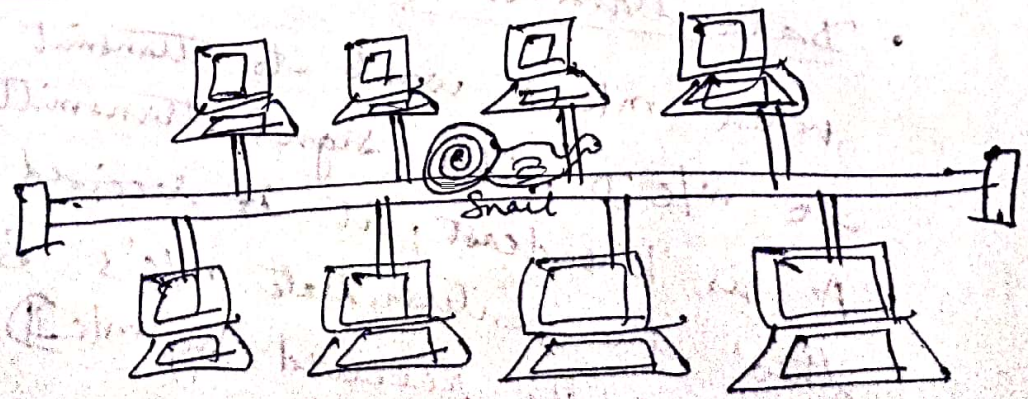


- when at least one terminator or the Bus is down, the whole network is affected. (Drawback)
- If one of the device (or m/c) is not working (defective) then it will not affect the entire n/w.



entire n/w works.
(Data transmission is not affected)
(failure of a device does not affect other devices)

Disadvantages



- when too many computers are connected with bus, the n/w can slow down.

Shubhangi K

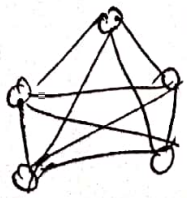
Advantages of Bus Topology

- Advantageous when the required n/w is small
- Easy to set up & easy to use [less difficulty] (easy installation)
- Costs less as compared to other topologies. (lower cable cost) or low implementation cost)
- Less space is required.
- Good and reliable for small network.
- Problem of Security (as message is broadcasted)
- Easy to add stations (devices)

Disadvantages:

- No Longer recommended
- Backbone breaks, whole n/w is down
- Limited number of devices can be attached
- Difficult to isolate problems
- Sharing same cable slows response rate.

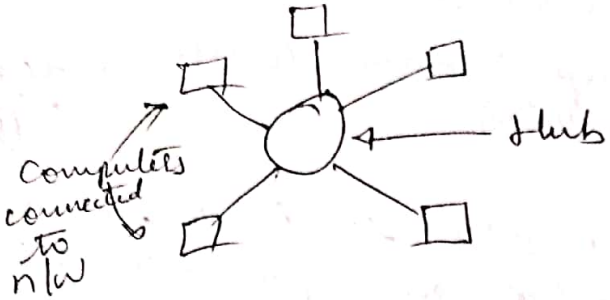
② Mesh Topology



- Point to point connections [privacy is maintained] ↳ advantage
- Every every is connected to every other node in the n/w
- Cable length increases & so the cost of installation [drawback]
- Each node should have multiple interfaces to get connected to other nodes in the n/w [drawback]
- not suitable when comm n computers in a building has to be connected to n computers in other building
- m x n cables are required. Large no of cables required to connect n nodes in mesh $\left(\frac{n(n-1)}{2}\right)$ If n=50 Then $\frac{50 \times 49}{2}$ = 1225 links
- So not suitable in LAN.

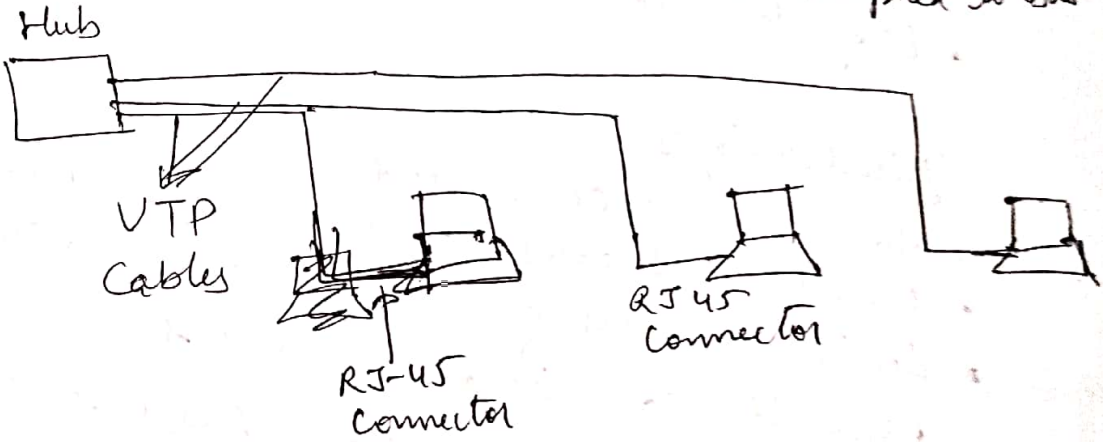
Shubhangi K

(3) Star Topology



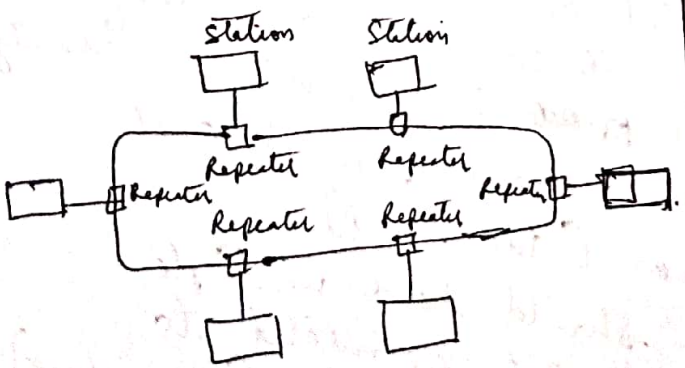
- centre of star is called Hub
- Connections are handled at one central point.
- Good quality of P2P connections.

Star Topology in practice (Much more reliable as compared to Bus

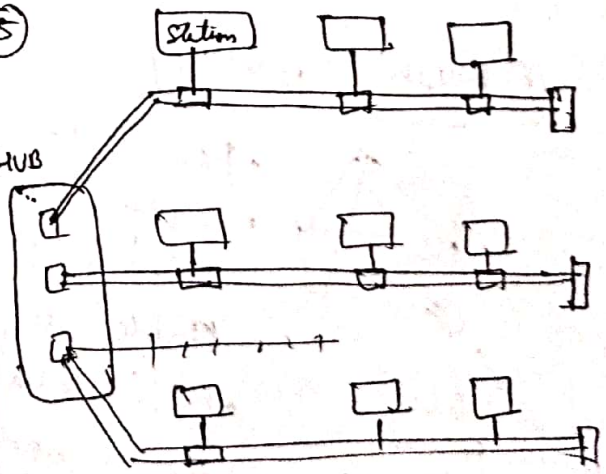


Extended Star Topology

(4) Ring Topology



(5)



Hybrid Topology: a star backbone with three Bus Networks.

Comparison of Network Topologies

Topology	Total No. of Links	Privacy	I/O lines with each device	Installation and Reconnection	Cost	Fault Identification and Isolation	Line configuration	Applications
Mesh	$\frac{n(n-1)}{2}$	yes	n-1	Difficult	Expensive	Easy	P2P	Regional Telephone offices
Star	n	No	one	Easy	Less Expensive	Easy	P2P	LANs, High Speed LANs
Bus	Single backbone with n drop lines	No	one	Difficult	Least Expensive	Difficult	Multi-Point	Not used in large networks
Ring	n	No	one	Easy	Moderate	Easy	Multipoint	IBM token ring. Not referred in todays LANs

Comparison of Network Topologies

n = no of nodes

P2P = Point to Point