Chapter-1
Introduction to Computer Network

Introduction: Computer Network

- A collection of computers and other devices that are connected together by communication channel for sharing information and resources is called computer network.
- The resources may include file, folder, disk drive, printer, scanner etc.
- **Internet** is an example of computer network i.e. network of network is called internet.
- Not all the nodes in the network are computers but are just network devices like switches, router etc. to facilitate communication.

Use/Applications of computer Network

- Exchange of information between different computers. (File sharing)
- Interconnecting small computers in place of large computers.
- Communication tools (voice, video)
- In distributed applications (Railway reservation system, Distributed databases etc.).
- Communication in mobile computers, such as laptop and handheld computers is possible through wireless networking.

Advantages of Computer network

- Better communication: Using computer network, different people can communicate with each other all over the world. People can communicate at low cost via email, chatting, telephone, SMS etc.
- Better resource sharing: In computer network, resources such as printer, scanner, fax machine etc. can be shared among different users.
- Data / application sharing: in a computer network, any authorized user can access data and applications stored on other computer in network.
- Inexpensive: We can interconnect multiple small computers in place of one large computer to increase the cost/performance ratio.
- For Back-up and Support—Networked computers can be used to take back-up of critical data

Disadvantages of Computer network

- Network Hardware, Software and Setup Costs
- Hardware and Software Management and Administration Costs
- Undesirable Sharing
- Data Security Concerns

Network Type

1. Local Area Network

- A LAN is privately owned network that operates within a single building like home, office, factory etc.
- A LAN is a computer network covering a small geographical area.
- LAN are perfect for sharing resources like printer, fax within a building but they can't connect distant sites.
- Wireless LAN is popular now a day in which wireless router act as access point.

2. Metropolitan Area Network

- A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN).
- A metropolitan area network, or MAN, consists of a computer network across an entire city, college campus or small region
- A MAN covers a city like Cable television network.
- A MAN is often used to connect several LANs together to form a bigger network.
- Recently developments in high speed wireless internet access have resulted in another MAN, which has been is popularly known as WIMAX (Worldwide Interoperability for Microwave Access).

3. Wide Area Network

- A WAN spans large geographical area, often a country or continent or entire world.
- In LAN, the hosts and subnets are owned and operated by a person or organization but in WAN, the hosts and subnets are owned and operated by different people or organizations
- The largest and most well-known example of a WAN is the Internet.
- WANs are used to connect LANs, MANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations

4. Personal Area Network

- PAN let devices communicated over the range of a person i.e. less than 2 meters.
- A common example is a wireless network that connect a computer with its peripherals.
- A sort range wireless network called Bluetooth helps to connect these components without wire.
- PANs also can be used to develop other technologies that communicate over short range such as RFID (Radio-Frequency Identification) on smart card.

5. Campus Area Network

- A MAN is often used to connect several LANs together to form a bigger network.
- When this type of network is specifically designed for a college campus, it is sometimes referred to as a campus area network, or CAN.

6. Global Area Network(GAN)

- A global area network (GAN) refers to a network composed of different interconnected networks that cover an unlimited geographical area.
- The term is loosely synonymous with Internet, which is considered a global area network.

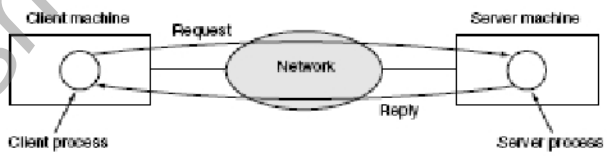
Differentiate LAN, MAN and WAN.

DISTINGUISH BETWEEN LAN,WAN,MAN

PARAMETERS	LAN	WAN	MAN
Ownership of network	Private	Private or public	Private or public
Geographical area covered	Small	Very large	Moderate
Design and maintenance	Easy	Not easy	Not easy
Communication medium	Coaxial cable	PSTN or satellite links	Coaxial cables, PSTN, optical fibre, cables, wireless
Bandwidth	Low	High	moderate
Data rates(speed)	High	Low	moderate

Network Application Architecture/Model

1. Client server architecture



- In computer network, the computer that we use on daily basis are often called as host or end system.
- Host are further divided into two categories: Client and server
- So a network in which certain computers have special dedicated task, providing services to other computer in the network is called client server network.
- Client are basically low end system i.e. desktop or workstation while server is powerful machine that provides services to requesting client.
- Services may include print service, file service, web service etc.
- In this architecture, the client process running on one end system request and receive information form server running on another end system.
- So client server model works on request response principle.
- Internet is based on client server architecture.

Advantage:

i. Security
ii. Central data location
iii. Easy to administer when network is large

iv. Network performance can be monitored

Disadvantage:

i. High cost due to central server
ii. Network administrator is required.
iii. If server is lost, data is also lost.

2. Peer to peer architecture

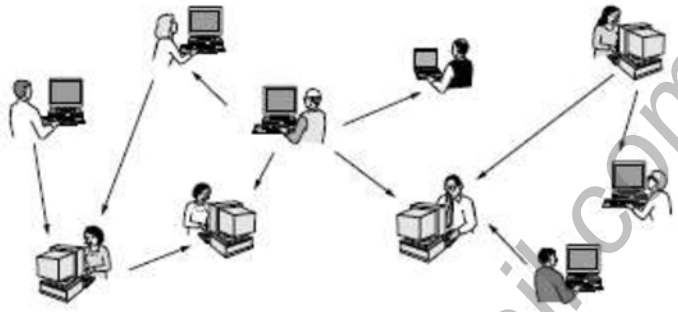


Figure 1-3. In a peer-to-peer system there are no fixed clients and servers.

- One of the simplest form of computer network is peer to peer network.
- Also called as p2p network.
- In this network, two or more end system are connected and share resources without going through a separate server computer.
- There is no dedicated server.
- The user at each workstation can decide which resources are shared on the network.
- In p2p network, all workstation are client and server at same time.
- Each workstation is connected with a simple and visible cabling system.
- The user then can administer their own computer and the resources they want to share on the network because each user is administrator of their own computer.
- However, it is less secured because anybody in the network can access any shared resource.

Advantage:

i. No need of central server, so is cheap.
ii. Sharing of data is easier.
iii. Backup of data.
iv. Shared administration.

Disadvantage:

i. Insecure.
ii. Complex of network is large.

3. Hybrid architecture

- Hybrid architecture are combination of p2p and client-server network.
- A common hybrid model is to have server that helps peers to find each other.
- This model provides better performance than both of the above model.
- One of the application that uses hybrid architecture is skype which used p2p for communication and also has centralized server as in client server model for finding address of remote party.

Network Topologies

- Topology is the physical layout of network or simply is the geometric arrangement of the computers in the network.
- The term topology refers to the way a network is laid out, either physically or logically.
- Physical topologies describe how the cables are installed.
- Logical topologies describe how the network messages travel.
- While physical topology refers to the way network devices are connected to cables and wires, logical topology refers to how the devices, cables and wires appear connected.

1. Bus Topology

- A bus is the simplest physical topology. It consists of a single cable that runs to every workstation
- This topology uses the least amount of cabling, but also covers the shortest amount of distance.
- If one device wants to send data to another device on the network, it puts message addressed to that device on the bus.

- A single computer is allowed to send data at one time.
- Here all the computers are connected serially one after another, so data will flow through all the intermediate computers, so each computer receive the data, check the address and if the address enclosed in data doesn't match then the computer reject the data and like this data flows to the next computer and the process continues till the destination computer receive the data after matching the address or end of cable is encountered.
- As the number of computer increases, the speed of the network starts decreasing.
- Terminator is used to close the ends.

Advantage of Bus Topology

- The bus is simple, reliable in small network, easy to use and easy to understand.
- The bus requires the least amount of cable to connect the computers together and is therefore is less expensive than other cabling arrangement.

Disadvantage of Bus Topology

- Computers can transmit at any time, and the computers on most bus network do not coordinate with each other to reserve times to transmit. So there is a chance of collision of data.
- The increase in number of computer decreases the speed of network considerably.
- A cable break or malfunctioning can bring the whole network down causing all network activity to stop.

2. Ring Topology

- Similar to bus except that the nodes are connected in a circle.
- First computer is connected to the last computer in the network.
- Each computer connects to two other computers, joining them in a circle creating a unidirectional path where messages move workstation to workstation.
- Each entity participating in the ring reads a message, then regenerates it and hands it to its neighbor until it arrives at its intended destination.
- This topology is found in peer-to-peer network.

Advantages of Ring Topology

- The fair sharing of the network resources.
- Suitable for small network.

Disadvantages of Ring Topology

- Failure of one computer on the ring can affect the whole network.
- It is difficult to troubleshoot the ring network.
- Adding and removing computers disrupts the network.

3. Star Topology

- Each computer on star network communicate with the central hub that resends the message either to all computers (broadcast) or only to destination computer.
- The hub can be active or passive.

- An active hub regenerates the electrical signal and sends it to all the computers connected to it. This type of hub is also called as multiport repeater.
- A passive hub only act as connector point and doesn't amplify or regenerate the signal. This type of hub does not require electrical power to run.

Advantages of Star Topology

- It is easy to modify and add new computers to a star network without disturbing the rest of the network.
- Single computer failure do not bring down the whole star network.
- Troubleshooting is easy in star network as hub can detect the network failure.

Disadvantages of Star Topology

- If the central hub fails, the whole network fails to operate.
- Star network require additional device at the central point to rebroadcast.

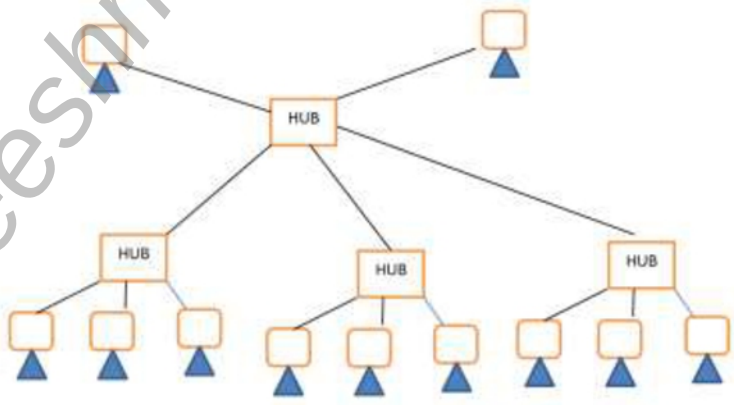
4. Tree Topology / Clustered Star Topology

- It is a variation of star topology.
- As in the star nodes, tree is also linked to central hub that control the traffic to other network.
- However not every device connects directly to the central hub.
- The central hub in the tree is called active hub.
- Multiple star networks central hub (secondary hub), which may be active or passive, are connected to the active hub of the tree.
- A good example of tree topology can be seen in cable TV technology where the main cable form the main office is divided into many branch and each branch is divided into smaller branches and so on. The hubs are used when a cable is divide.

Advantages of Tree Topology

The advantages of tree topology is similar to that of star topology however the addition of secondary hub provides following advantages.

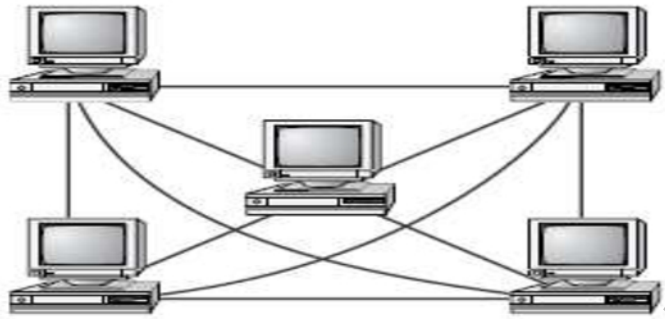
- It allows more device to be attached into a single central.
- Since the central hub is active, it increases the distance a signal can travel between the large number devices.
- It allows network to isolate and prioritize communications on different computer.



5. Mess Topology

- The mesh topology is the simplest logical topology in terms of data flow, but it is the most complex in terms of physical design.
- In this physical topology, each device is connected to every other device
- This topology is rarely found in LANs, mainly because of the complexity of the cabling.

- If there are N computers, there will be (N × (N−1)) ÷ 2 cables in the network. For example, if you have five computers in a mesh network, it will use 5 × (5 − 1) ÷ 2, which equals 10 cables.
- The complexity of cabling is compounded when you add another workstation.
- Example: Internet is a mesh network



Advantage

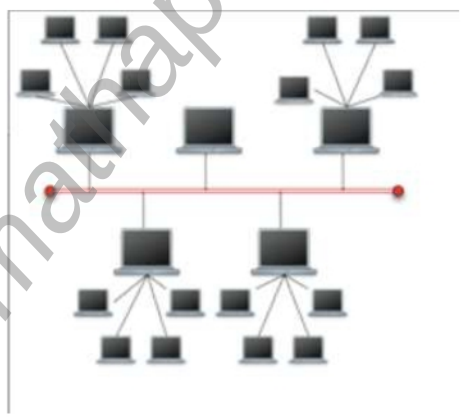
- Cables must be run from each device to every other device. The advantage you gain from it is its high fault tolerance.
- With a logical mesh topology, however, there will always be a way of getting the data from source to destination.

Disadvantages

- Lots of cable so the physical mesh topology is very expensive to install and maintain.
- Hard to setup
- Troubleshooting is extremely difficult

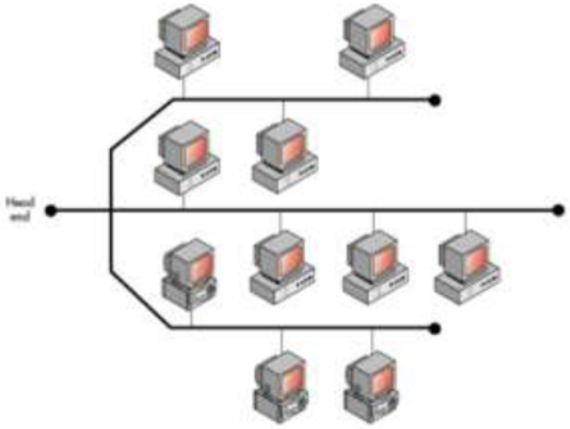
5. Hybrid Topology

- Hybrid networks use a combination of any two or more topologies in such a way that the resulting network does not exhibit one of the standard topologies (e.g., bus, star, ring, etc.).
- A hybrid topology is always produced when two different basic network topologies are connected. One common examples for Hybrid network is Star bus network.
- A Star Bus network consists of two or more star topologies connected using a bus trunk (the bus trunk serves as the network's backbone).



6. Distributed Bus Topology

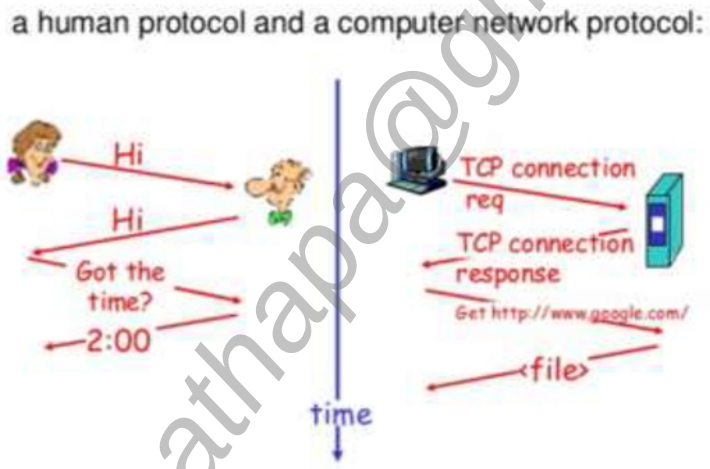
- In simple or linear bus topology, all the nodes of the network are connected to a common transmission medium which has exactly two endpoints.
- In distributed bus topology, all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium.
- When the cable(trunk) branches, the division is made by means of a simple connector. This topology is susceptible to bottlenecking and single-point failure.



- The physical distributed bus topology functions is exactly the same fashion as the physical linear bus topology (i.e., all nodes share a common transmission medium).

Protocols and Standards

- Protocols are the set of rules that govern all activity in the network that involves two or more communicating remote entities.
- Protocols are running everywhere in the network.
- Example: protocol in router determine a packet path from source to destination, error detection protocol could detect the transmission error etc.



Protocol Stack , Interfaces and Services

- Protocols are the set of rules that govern all the activity in the network that involves two or more communication entities.
- To reduce the design complexities, network designers organize the protocols, network hardware and software that implement the protocol in layers.
- A protocol in one layer perform a certain set of operations on data, the data is then passed to the next layer where another protocol perform different set of operations. I.e. each layer provides certain services to upper layer.

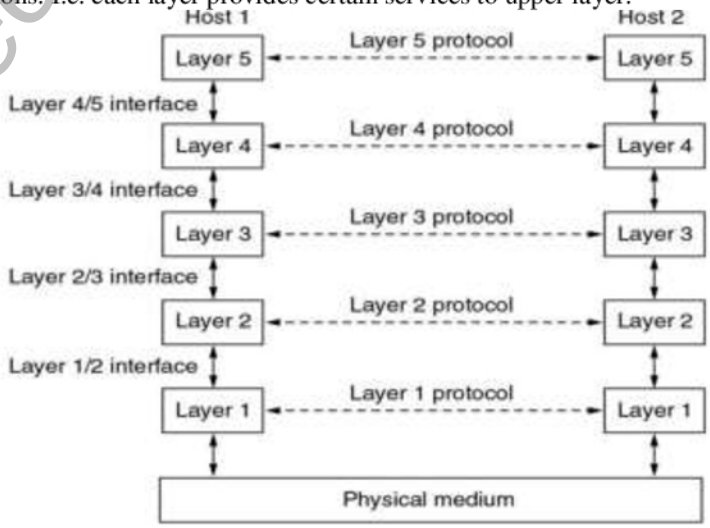


Fig 1: layer, services and interfaces

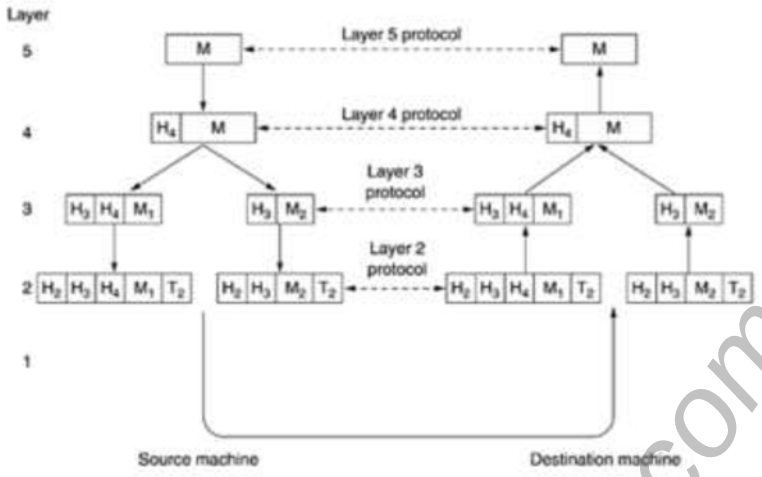


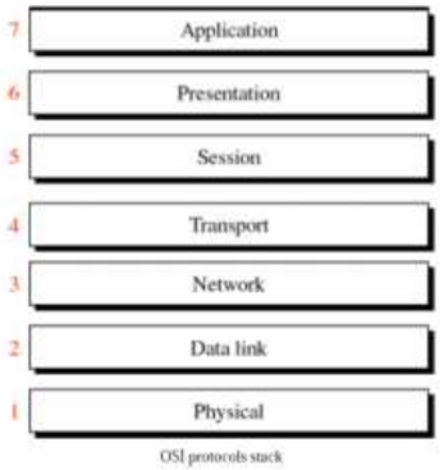
Fig 2: Example information flow supporting virtual connection in layer 5

- The protocols at various layer are called protocol stack.
- The key concept of protocol stack is each n-1 layer provides service to upper layer n.
- These layers communicate with each other by exchanging n-message. These message are called layered-n protocol data unit or n-PDU.
- Between each pair of layer is an interface that define the services the lower layer provides to upper one.
- Example: The application-to-transport interface defines how application programs make use of the transport layers. For example, this interface level would define how a web browser program would talk to TCP/IP transport software
- In above figure 2, the source generates message in layer 5 and passed down to layer 4. This layer 4 put some header in front of message to obtain 4-PDU. Then this message is passed down to layer3. In layer 3, 4-PDU is divided into two parts M1 and M2 and additional header is appended in front of message. The header may include control information such as sequence number to allow peer layer 3 on destination to deliver message on right order. Simply header contains additional information needed by the sending and receiver side.
- The procedure continues in the source, adding more header at each layer until 1-PDU are sent to the destination over a physical link.
- At the other end, the destination host receive 1-PDU and direct them up the protocol stack. At each layer, the corresponding header is removed.
- Finally, Message M is obtained from M1 and M2 and then passed to destination application.

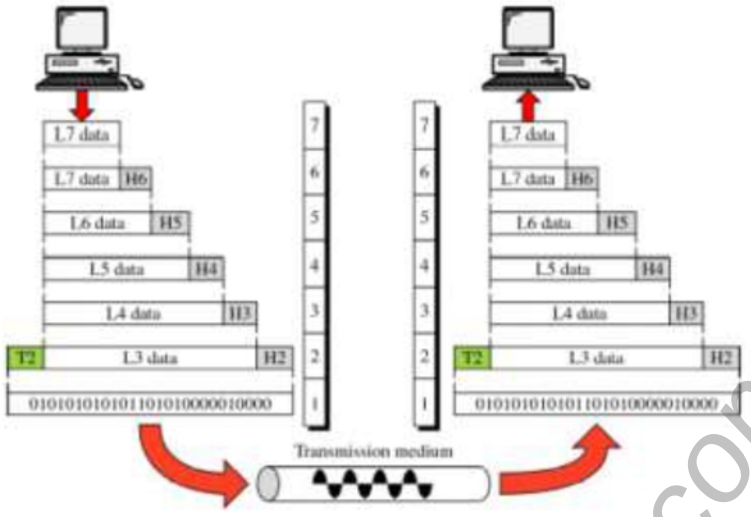
Drawback of Layer approach

1. Possibility of redundancy of functionality
2. Dependency of one layer to another violate the goal of separation of layers.

The OSI Reference Model



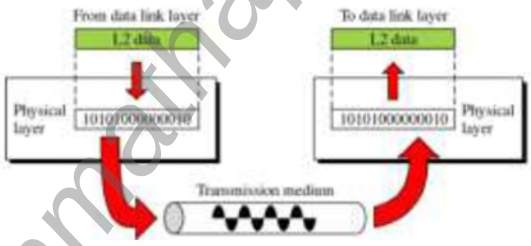
OSI protocols stack



- Appeared after TCP/IP model.
- The international organization for standardization (ISO) has developed OSI (open system interconnection) model in 1977.
- An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- In order for computer communicate, there must be some rules, followed by the computer for transferring information from one computer to another.
- OSI model, simple define which task need to be done and which protocol will handle those tasks at each of the seven layers of the model. These all layers are present in each computer logically; all the information before transferring has to be processed under the seven layers.
- At each layer (except layer 7 and 1) in the sender side, a header is added to the data unit received from the upper layer. At the layer 2, a trailer is added as well.
- As each block of data reaches the next higher layer in receiving end, the header and trailer attached to it at the corresponding layer at the sending device are removed, and actions appropriate to that layer are taken.

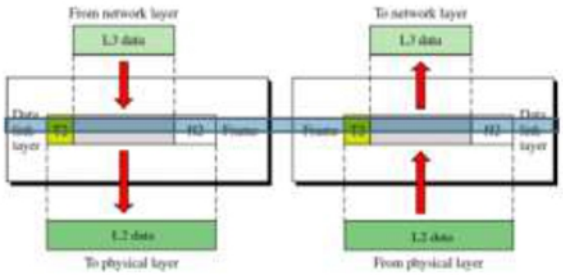
Layers in OSI model

1. **Physical Layer**



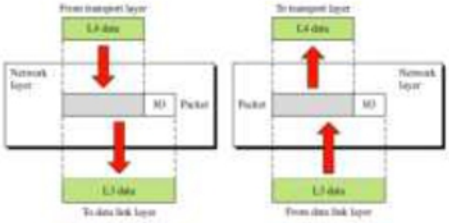
- This layer is used for sending bits 1's or 0's from one computer to another computer.
- It also deals with the physical connection between the computers. It mainly transmits and receives the signal.

2. **Data Link Layer**



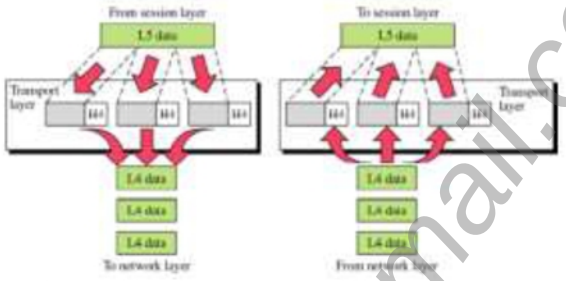
- The data link layer provides for the delivery of data over a single link from one device to another in the route and device decided by the network layer.
- The data link layer is responsible for correcting transmission errors induced during transmission.
- This is achieved by the data link layer by performing the tasks like framing(encapsulation), flow control, error control, access control, and physical addressing.

3. Network Layer



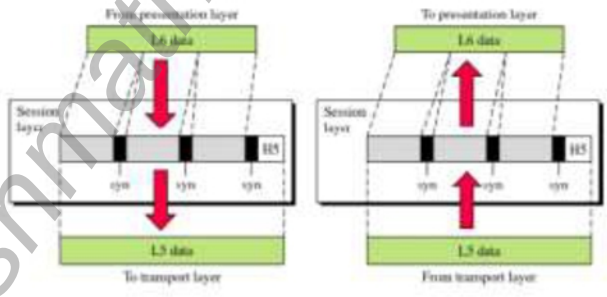
- The network layer is responsible for the source-to-destination delivery of a packet possibly across multiple networks.
- So the network layer is responsible for deciding route and forwarding the packets to a particular device.
- For this it uses two protocol i.e. IP and routing protocol. IP for translating logical network address to physical machine address. Routing protocols are used to determine the path for the packet if there are several ways a packet can get to its destination.

4. Transport Layer



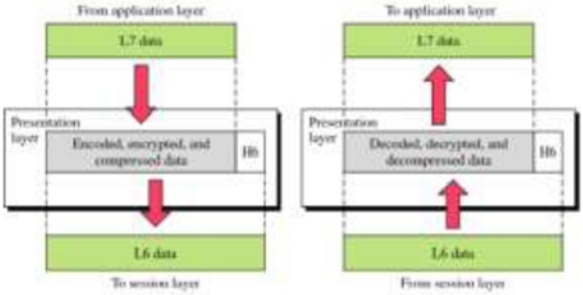
- This layer is responsible for delivering error free data to destination computer.
- This layer breaks the large message into small packets and then sends these packets to the destination computer. The transport layer also sends acknowledgement to the sender that message has been sent successfully i.e. the transport layer ensures data is successfully sent and received between two end systems. If data is sent incorrectly, this layer has the responsibility to ask for retransmission of the data.
- Also it ensures data are passed onto the upper layers in the same order in which they were sent.
- It also provides multiplexing/DE multiplexing for combining data from several source for transmission over a single data path.
- Congestion control is also provided by this layer.
- The Transmission Control Protocol (TCP) of the TCP/IP protocol suite resides at the transport layer.

5. Session Layer



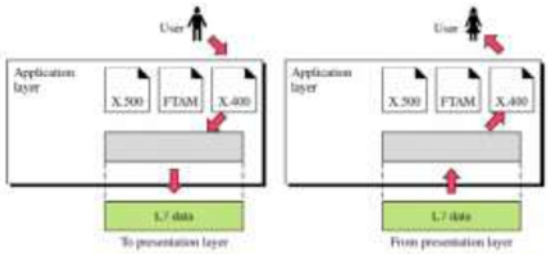
- It is responsible for the session between computers to be established and terminated.
- It provides two systems into a dialog to find each other and provide a common link.
- Also, the session layer organizes and synchronizes the exchange of data between application processes. I
- t works with the application layer to provide simple data sets called synchronization points that let an application know how the transmission and reception of data are progressing.
- In simplified terms, the session layer can be thought of as a timing and flow control layer.

6. Presentation Layer



- This layers translates the information between the format the network requires and the format the computer expects.
- The presentation layer is responsible for task like data translation (e.g. converting to ASCII coded file or XML file), compressions, encryption etc.

7. Application Layer



- The application layer is the topmost layer of OSI model.
- It provides services that directly user application such as webpage, email, file transfer etc. it uses many protocols including HTTP to support web, SMTP to support email, FTP to support file transfer, DNS etc.

Summary

Summary:
Physical Layer: How to transmit bits.
Data Link Layer: How to transmits frames
Network: How to route packets to the node.
Transport: How to send packets to the applications.
Session: Manage connections.
Presentation: Encode/Decode messages, security.
Application: Everything else.

Benefits of OSI model

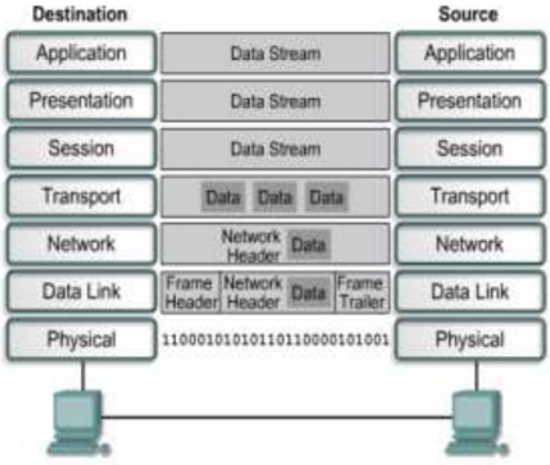
- It breaks network communication into smaller, more manageable parts.
- It standardizes network components to allow multiple vendor development and support.
- It allows different types of network hardware and software to communicate with each other.
- It prevents changes in one layer from affecting other layers.
- It divides network communication into smaller parts to make learning it easier to understand.

Protocols in TCP/IP and OSE

TCP/IP	OSI Model	Protocols
Application Layer	Application Layer	DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP, POP3, RTP, RTSP, SSH, SIP, SMTP, SNMP, Telnet, TFTP
	Presentation Layer	JPEG, MIDI, MPEG, PICT, TIFF
	Session Layer	NetBIOS, NFS, PAP, SCP, SQL, ZIP
Transport Layer	Transport Layer	TCP, UDP
Internet Layer	Network Layer	ICMP, IGMP, IPsec, IPv4, IPv6, IPX, RIP
Link Layer	Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring
	Physical Layer	Bluetooth, Ethernet, DSL, ISDN, 802.11 Wi-Fi

Data Encapsulation

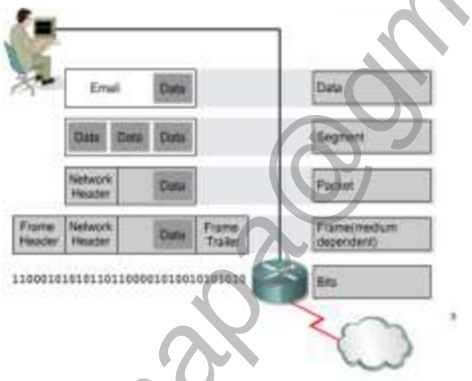
- All communications on a network originate at a source, and are sent to a destination.
- The information sent on a network is referred to as data or data packets.
- If one computer (host A) wants to send data to another computer (host B), the data must first be packaged through a process called encapsulation.
- Encapsulation wraps data with the necessary protocol information before network transit.
- Therefore, as the data packet moves down through the layers of the OSI model, it receives headers, trailers, and other information.



Example:

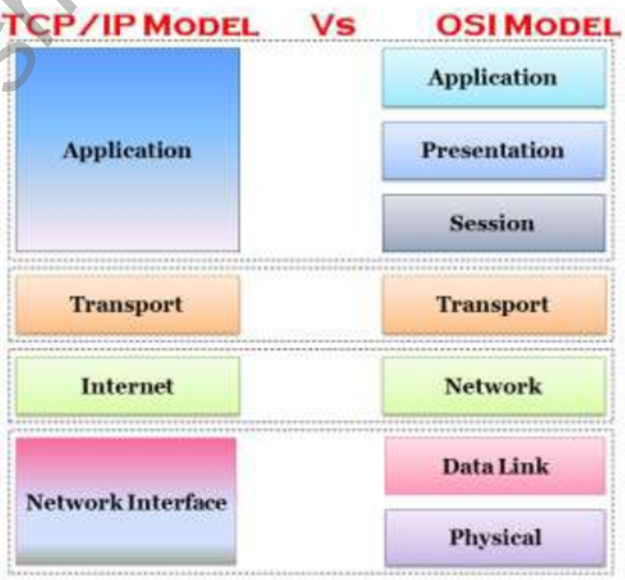
Perform the following five conversion steps in order to encapsulate the data.

1. Build the data.
2. Package the data for end-to-end transport.
3. Add the network IP address to the header.
4. Add the data link layer header and trailer.
5. Convert to bits for transmission.



TCP/IP Reference Model

- The ARPANET was a research network sponsored by the DOD (U.S Department of Defense).
- It had connected hundreds of universities and government installations using leased telephone lines. When satellite and radio networks were added later, the existing protocols had trouble inter working with them, so new reference architecture was needed.
- Thus, the ability to connect multiple networks together without facing any problem was one of the major design goals from the very beginning. This architecture later became known as TCP/IP Reference Model.
- This model basically consists of four main layers as describe in figure



1. Application layer:
- On top the transport layer is the application layer. TCP/IP combines the OSI application, presentation, and session layers into its application layer.
- The application layer handles high-level protocols, representation, encoding, and dialog control.
- The TCP/IP protocol suite combines all application related issues into one layer. It ensures that the data is properly packaged before it is passed on to the next layer. TCP/IP has protocols to support file transfer i.e. FTP, e-mail i.e. SMTP, DNS, and remote login etc.

2. Transport Layer:
- The transport layer ensures that packets are delivered error free, in sequence and with no losses or duplication.
- The transport layer breaks large message from the upper layer application into packet to be sent to the destination computer and again on receiving site resembles packet into the message to be presented to the application layer.
- The transport layer typically sent an acknowledgement to the originator for message received.
- Two end to end protocols have been defined here.
- The first one, TCP (Transmission Control Protocol) is a reliable connection oriented protocol that allows a byte stream originated on one machine to be delivered without error on any other machine in the internet.
- The second protocol in this layer, UDP (User Datagram Protocol), is unreliable, connectionless protocols for applications that do not want TCP's sequencing or flow control and wish to provide their own. It is also widely used for one-shot, client-server type request reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video.

3.Internet Layer
- The main job of this layer is to inject packet into any network and have them travel independently to the destination.
- The main protocol that function at this layer is IP. Best path determination and packet switching occurs at this layer.

4. Network Access:
- The network access layer allows an IP packet to make a physical link to the network media.
- It includes all the detail include in OSI data link and physical layer.
- Drivers for software applications, modem cards, and other devices operate at the network access layer. The network access layer defines the procedures used to interface with the network hardware and access the transmission medium.
- Other protocols that operate at this layer are ARP, RARP etc.

Comparison of OSI Model and TCP/IP Model:

The OSI and TCP/IP models have many similarities:
- Both are based on layers' concept.
- Both have application layers, though they include different services.
- Both have comparable transport and network layers.
- Both use packet-switched instead of circuit-switched technology.
- Networking professionals need to know both models.

Here are some differences of the OSI and TCP/IP models:
- TCP/IP combines the OSI application, presentation, and session layers into its application layer.
- TCP/IP combines the OSI data link and physical layers into its network access layer.
- TCP/IP appears simpler because it has fewer layers.
- When the TCP/IP transport layer uses UDP it does not provide reliable delivery of packets. The transport layer in the OSI model always does.

OSI MODEL	TCP/IP MODEL
Contains 7 Layers	Contains 4 Layers
Uses Strict Layering resulting in vertical layers.	Uses Loose Layering resulting in horizontal layers.
Supports both connectionless & connection-oriented communication in the Network layer, but only connection-oriented communication in Transport Layer	Supports only connectionless communication in the Network layer, but both connectionless & connection-oriented communication in Transport Layer
It distinguishes between Service, Interface and Protocol.	Does not clearly distinguish between Service, Interface and Protocol.
Protocols are better hidden and can be replaced relatively easily as technology changes (No transparency)	Protocols are not hidden and thus cannot be replaced easily. (Transparency) Replacing IP by a substantially different protocol would be virtually impossible
OSI reference model was devised before the corresponding protocols were designed.	The protocols came first and the model was a description of the existing protocols

- The Internet was developed based on the standards of the TCP/IP protocols. The TCP/IP model gains credibility because of its protocols. The OSI model is not generally used to build networks. The OSI model is used as a guide to help students understand the communication process.

Connection Oriented and Connection less service

- In computer network, the links, routers and other pieces of the Internet provide the means to transport these messages between the end system applications.
- The Internet, and more generally TCP/IP networks, provide two types of services to its applications: connectionless service and connection oriented service.
- So a developer creating an internet application like email, file transfer, web sites must program the application to use one of these services.

i. **Connection oriented service**
   - When an application uses the connection oriented service, the client and server residing in different end system sends control packet to each other before sending packets with real data.
   - The procedure of sending control packet is also called as handshaking that alert the client and server to be read for transmission of packets.
   - Once handshaking is finished, a connection is established between two end system hence called as connection oriented.
   - The connection oriented service provides other service like reliable data transfer, flow control, congestion control.
   - The connection oriented service is provided by transport layer protocol called TCP i.e. transmission control protocol.
   - Internet application like FTP, HTTP, SMTP etc. uses connection oriented service

ii. **Connectionless service**
   - In connection less service, when one side of an application wants to send packets to another side of an application, the sending application simply sends the packet without handshaking.
   - Since there in no handshaking procedure prior to the transmission of packets, data can be delivered faster.
   - But there is no acknowledgement either, so a source never knows for sure which packets arrive in destination.
   - This service also has no provision for flow control, congestion control.
   - The connectionless service is provided by transport layer protocol called UDP i.e. user datagram protocol.
   - Internet application like internet telephony, video chatting etc. uses connection oriented service

Connection Oriented Vs Connectionless service

Criteria	Connection-Oriented	Connection-Less
Connection	Prior connection needs to be established.	No prior connection is established.
Resource Allocation	Resources need to be allocated.	No prior allocation of resource is required.
Reliability	It ensures reliable transfer of data.	Reliability is not guaranteed as it is a best effort service.
Congestion	Congestion is not at all possible.	Congestion can occur likely.
Transfer mode	It can be implemented either using Circuit Switching or VCs.	It is implemented using Packet Switching.
Retransmission	It is possible to retransmit the lost data bits.	It is not possible.
Suitability	It is suitable for long and steady communication.	It is suitable for bursty transmissions.
Signaling	Connection is established through process of signaling.	There is no concept of signaling.
Packet travel	In this packets travel to their destination node in a sequential manner.	In this packets reach the destination in a random manner.
Delay	There is more delay in transfer of information, but once connection established faster delivery.	There is no delay due absence of connection establishment phase.

Internet

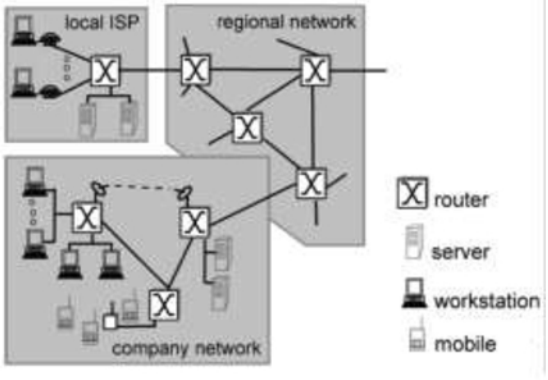


Fig: Some Piece of Internet

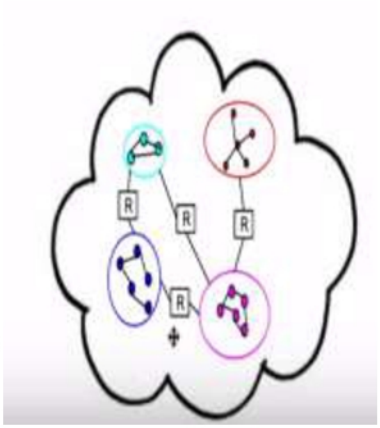


Fig: Internet as Network of Network

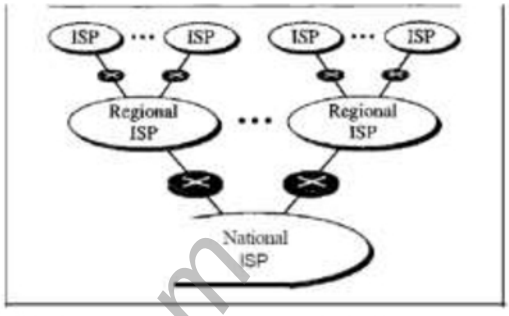


Fig: ISP structure

- The public Internet is a world-wide computer network that interconnects millions of computing devices throughout the world.
- Internet connects traditional devices like desktop PCs, servers as well as modern devices such as Web TVs, mobile computers etc. All of these devices are called hosts or end systems.
- The Internet applications such as WWW (a network of online content that is formatted in HTML and accessed via HTTP) and e-mail, are network application programs that run on such end systems.
- End systems are governed by protocols that control the sending and receiving of information within the Internet. TCP (Transmission Control Protocol) and IP (the Internet Protocol) are two of the most important protocols in the Internet. The Internet's principle protocols are collectively known as TCP/IP protocols.
- End systems are connected together by communication links. Communication link can be wired or wireless.
- End system are indirectly connected to each other through intermediate switching devices known as routers.
- Rather than provide a dedicated path between communicating end systems, the Internet uses a technique known as packet switching that allows multiple communicating end systems to share a path, or parts of a path, at the same time.
- The topology of the Internet, i.e., the structure of the interconnection among the various pieces of the Internet, is loosely hierarchical. In term of bottom-to-top, the hierarchy consists of end systems connected to local Internet Service Providers (ISPs) though access networks i.e. LAN, telephone line, mobile network. Local ISP's are in turn connected to regional ISPs, which are in turn connected to national and international ISPs. The national and international ISPs are connected together at the highest tier in the hierarchy. ISPs are also called as internet backbone.