1.1 Uses of Computer Network
1.2 Networking model : client/server, p2p, active network
1.3 Protocols and Standards
1.4 OSI model and TCP/IP model
1.5 Comparison of OSI and TCP/IP model
1.6 Example network: The Internet, X.25, Frame Relay, Ethernet, VoIP, NGN and MPLS, xDSL.

A computer network is an interconnection of various computers to share software, hardware, resources and data through a communication medium between them.

Any Computer Networking communication need a sender, a receiver and a communication medium, protocols and operating system to establish networking and to transfer signal or Data from sender to the receiver.

A networks model describes the organization of various computers in a network for using resources.

Networks provide the benefits of *exchanging information or Data, sharing resources, reducing system costs, increased reliability and flexible working environment*.

Chronology of significant computer-network developments

- late 1950s, early networks of computers included the U.S. military radar system
- In 1960, the commercial airline reservation system went online with two connected mainframes.
- 1965, Western Electric introduced the first widely used telephone switch that implemented true computer control.
- 1969, the first four nodes of the ARPANET were connected using 50 kbit/s circuits
- In 1972, commercial services using X.25 were deployed
- 1973, Robert Metcalfe wrote a formal memo at Xerox PARC describing Ethernet,
- 1995, the transmission speed capacity for Ethernet increased from 10 Mbit/s to 100 Mbit/s
- 1998, Ethernet supported transmission speeds of a Gigabit. Subsequently, higher speeds of up to 100 Gbit/s were added (as of 2016)

Computer Network Model

A **computer networks** communication can be based on centralized, distributed or collaborative computing. *Centralized computing* involves many workstations or terminals, connected to one central mainframe or another powerful computer. *Distributed computing* interconnects one or more personal computers and allows various services like Data sharing, hardware sharing resources sharing or network sharing. *The collaborative computing* is the combination of centralized and distributed computing.

1. *Centralized computing.*

• It is also known as client-server computing.
• In this type of system, multiple computers are joined to one powerful mainframe computer.
• The server or mainframe computer has huge storage and processing capabilities.
• The computers that are connected to the mainframe or server are called Clients or Nodes.
• These nodes are *not* connected to each other; they are only connected to server.

2. *Distributed computing*

• If one computer can forcibly start, stop or control another the computers are not autonomous.

A system with one control unit and many slaves, or a large computer with remote printers and terminals is not called a computer network, it is called a **Distributed System**.

• Distributed computing means that the task is divided among multiple computers.
• Distributed computing interconnects one or more personal computers or Workstations.

3. *Collaborative computing / Hybrid computing*

• It is the combination of centralized and distributed computing

• In collaborative computing, the nodes are able to serve the basic needs of their users but they are dependent on some other computers for processing some specific request.

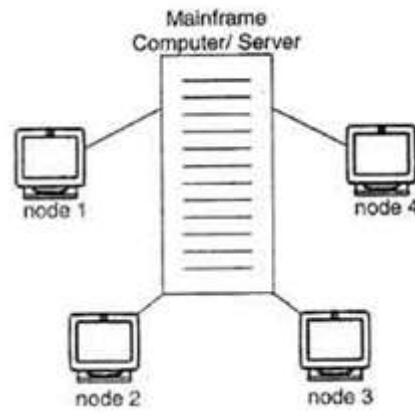


Fig. Centralized Computing

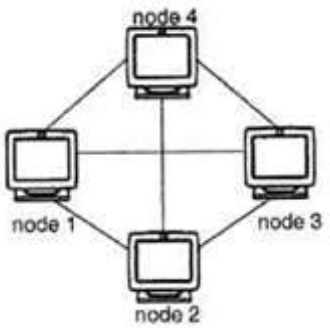


Fig. Distributed Computing

Computer Network Classification

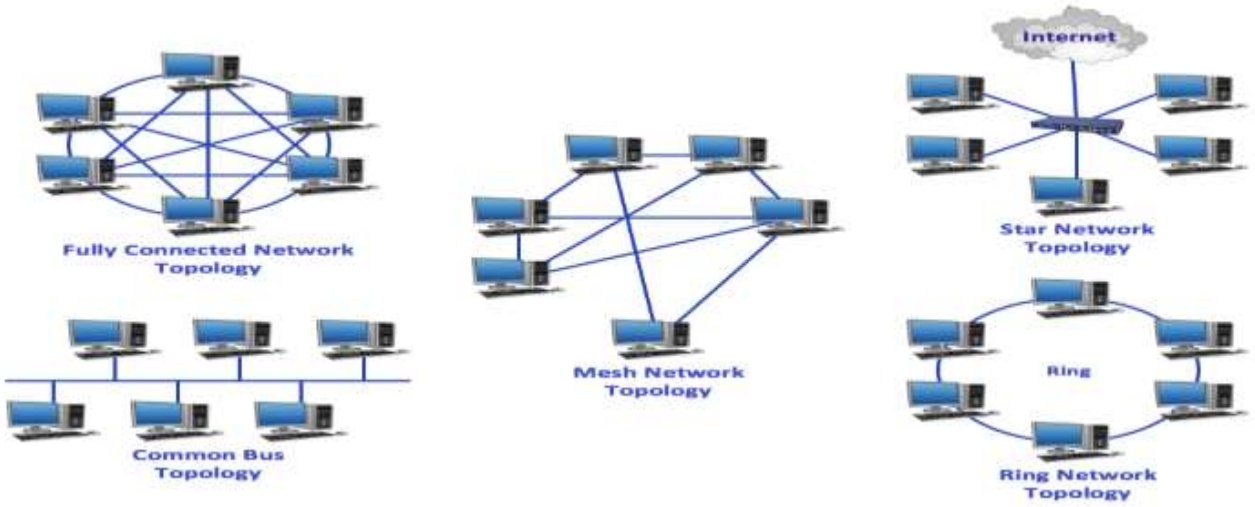
The local area network communication can be constructed by using server based model or peer to peer model. In peer to peer networks, the individual clients share data and resources but no one computer is treated as server.

LAN : Local area network is the small network that cover a small area of Network.
MAN : Metropolitan area networks are created by combining various local area networks.
WAN : Wide area networks are the biggest networks that provide connectivity across the globe.

Computer Network topology

The physical arrangement of computers in a communication network is called as topology.

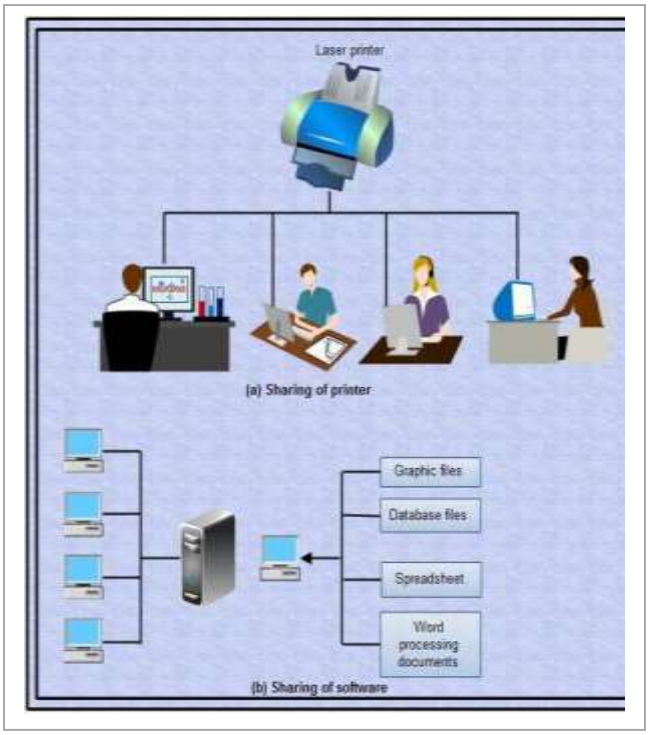
Star topology: every system on the network is connected to a central controller called Hub and all the data is transmitted through this. Star topology is very easy to install and configure.
Bus topology: a single cable acts as a backbone of the communication network and all the nodes or computers are attached to it by using T connectors.
Ring Topology : Failure of one computer disturbs the whole network.
Mesh Topology : some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
Fully Connected Network Topology : All devices or nodes are connected to each other.



1.1 Uses of Computer Networks

The computer networks are playing an important role in providing services to large organizations as well as to the individual common man.

• Many organizations have a large number of computers in operation. These computers may be within the same building, campus, city or different cities. Even though the computers are located in different locations, the organizations can track of inventories, monitor productivity, do the ordering and billing etc.



• The computer networks are useful to the organizations in the following ways:

1. Resource and Information sharing e.g. printer, software, file, video etc.
2. Data Protection: *For providing high reliability.*
3. Cost effective.
4. Communication and Collaboration: *It can provide a powerful communication medium.*
5. Security System
6. E-Commerce
7. Mobile Users

1. Resource and Information sharing

• It allows resources(e.g. printers, files) or same devices sharing to *anyone on the network irrespective of the physical location* of the resource and the user.
• Show in Fig (a) and (b) which shows a printer being shared and different information being shared.
•Information sharing is the exchange of data between various organizations, people, and technologies. Different information and data can be shared like the file, videos, etc.

2. Data Protection: *High reliability due to alternative sources of data*

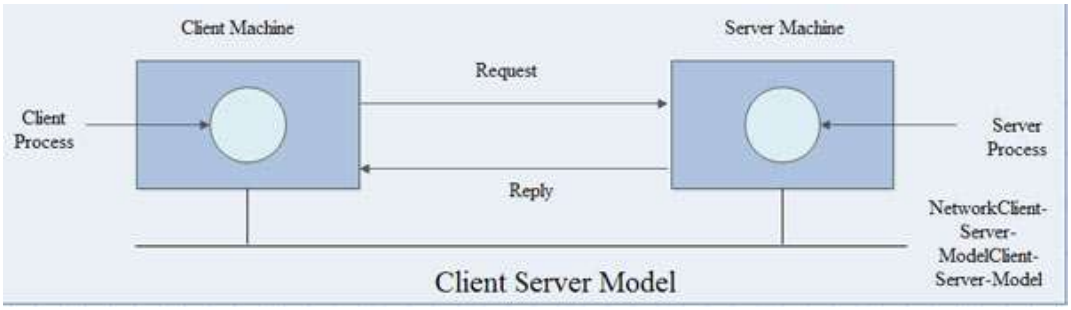
• It provides high reliability by having alternative sources of data. For e.g. all files could be replicated on more than one machines, so *if one of them is unavailable due to hardware failure or any other reason, the other copies can be used.*
• The aspect of high reliability is very important for military, banking, air traffic control, nuclear reactor safety and many other applications where continuous operations are a must even if there are hardware or software failures.

3. Cost effectivie

• Computer networking is an important financial aspect for organizations because it saves money.
• Organizations can use separate personal computer one per user instead of using mainframe computer which are expensive.

• The organizations can use the workgroup model (**peer to peer)** in *which all the PCs are networked together and each one can have the access to the other for communicating or sharing purpose.*

• The organization, if it wants security for its operation, it can go in for the **domain model** in which there is a server and clients. All the clients can communicate and access data through the server. The whole arrangement is called as **client -server model.**



4. Communication medium: *Communication and Collaboration*

• A computer network provides a powerful communication medium among widely separated employees.

• Using network it is easy for two or more employees, *who are separated by geographical locations to work on a report, document or R and D simultaneously i.e. on -line.*

Networks **for People:**

• Starting in 1990s, the computer networks began to start delivering services to the private individuals at home.

• The computer networks offer the following services to an individual person:

1. Access to remote information
2. Person to person communication
3. Interactive entertainment.

1. Remote Access: *Access to remote information*- Access to remote information involves interaction· between a person and a remote database. Access to remote information comes in many forms like:

(i) Home shopping, paying telephone, electricity bills, e-banking, on line share market etc.

(ii) Newspaper is. On-line and is personalized, digital library consisting of books, magazines, scientific journals etc.

(iii) World wide web which contains information. about the arts, business, cooking, government, health, history, hobbies, recreation, science, sports etc.

2. Person to person communication: Person to person communication includes:

(i) Electronic-mail (e-mail)

(ii) Real time e-mail i.e. video conferencing allows remote users to communicate with no delay by seeing and hearing each other. Video-conferencing is being used for remote school, getting medical opinion from distant specialists etc.

(iii) Worldwide newsgroups in which one person posts a message and all other subscribers to the newsgroup can read it or give their feedbacks.

3. Interactive entertainment: Interactive entertainment includes:

(i) Multiuser real-time simulation games.

(ii) Video on demand.

(iii) Participation in live TV programs likes quiz, contest, discussions etc.

In short, the ability to merge information, communication and entertainment will surely give rise to a massive new industry based on computer networking.

What is Real-time TV program and Live TV program?

5. Security

(i) Surveillance System

(ii) Security alarm system

(iii) Location tracker system

(iv) SMS system

(v) Realtime Geographical Information System

6. E-commerce:- Computer Network is also used in E-commerce where users can pay bills, transfer cash, buy good, etc using the computer.

7. Mobile Users :- Computer Network is used in the mobile device like telephone, Smartphone, tablets, etc for communication, the internet, file sharing, etc.

1.2 Network Model : *organization of various computers in a network for using resources.*

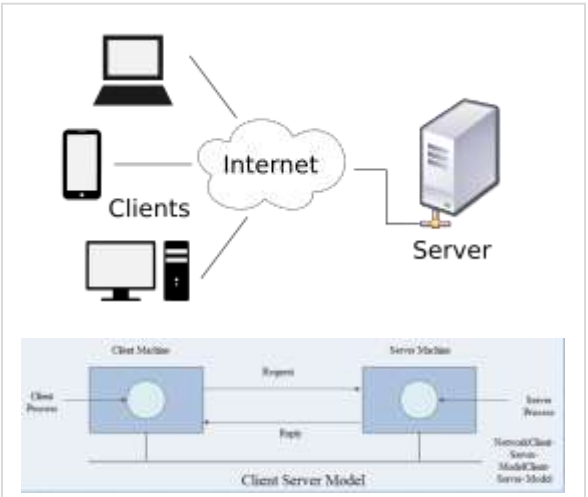
***Client Server**

Client or Host or service requester : The *individual workstations or pc* in the network are called as clients which request for services.

Server or service providers: The *central computer or stable/static host* which is more powerful than the clients and which allows the clients to access its software and database is called as the server.

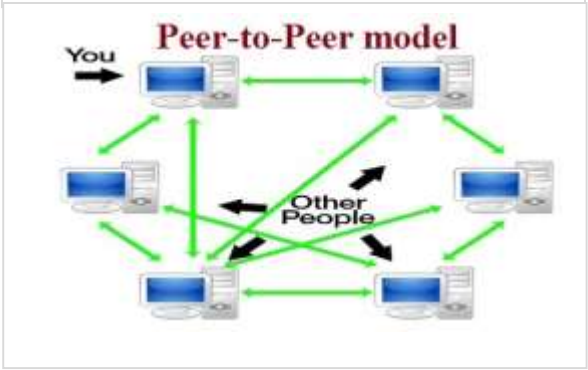
The **client–server model** is a distributed application structure but centralized system that partitions *tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients.* Often clients and servers communicate over a computer network on separate hardware, but both client and server may reside in the same system.

A server host runs one or more server programs which share their resources with clients. A client does not share any of its resources, but requests a server's content or service function. Clients therefore initiate communication sessions with servers which await incoming requests. *Examples of computer applications that use the client–server model are Email, network printing, network antivirus, and the World Wide Web.*

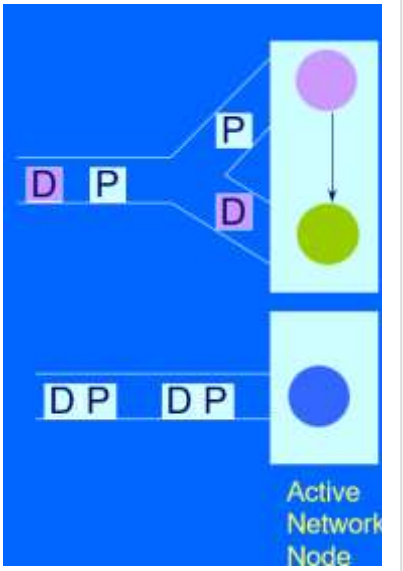


***P2P : Peer-to-peer (P2P)** computing or networking is a distributed application architecture that partitions *tasks or workloads between peers or nodes*. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes. *Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts.* Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model in which the consumption and supply of resources is divided.

A peer-to-peer (P2P) network is created when two or more PCs or devices are connected and share their resources without communicating with a separate server computer. In peer to peer networking architecture, each computer (workstation) has equivalent capabilities and responsibilities. Each PC acts as an independent workstation that stores data on its own hard drive but which can share it with all other PCs on the network. *Computers connecting with each other in a workgroup can share files, printers, and internet access.*



***Active Network or SDN(Software Defined Network):** Active networks is highly programmable networks (*A programmable network is one in which the status/ behavior of network devices and flow control- is the management of data flow between computers or devices or between nodes in a network so that the data can be handled at an efficient step. is handled by software,* that operates independently from network hardware.*)* that perform computations on the user data that is passing through them.



- ✓ An active network is a network in which the nodes are programmed to perform custom operations on the messages that pass through the node. For example, a node could be programmed or customized to handle packets on an individual user basis or to handle multicast packets differently than other packets
- ✓ Active networking allows the possibility of highly tailored and rapid "real-time" changes to the underlying network operation.
- ✓ Active networking places computation within packets traveling through the network. Software-defined networking decouples the system that makes decisions about where traffic is sent (the control plane) from the underlying systems that forward traffic to the selected destination (the data plane).

We distinguish two methods to active networks, discrete and integrated, depending on whether programs and data are carried discretely, i.e., within separate messages, or in an integrated fashion.

Active networks allow an individual user, or groups of users, to inject customized programs into the nodes of the network.

Contains both your data, and the program, the printer runs to print your data

Packet == data + code

Two Models of Active Networks (ANs)

Active networks are active in two ways :-

- *Programmable switches: discrete ANs*

– Separation of program loading and execution E.g. program loading only by network operator
– Packet is demultiplexed to the right program
– Programs (P) Injected into Active Nodes Separately from Passive Data (D)

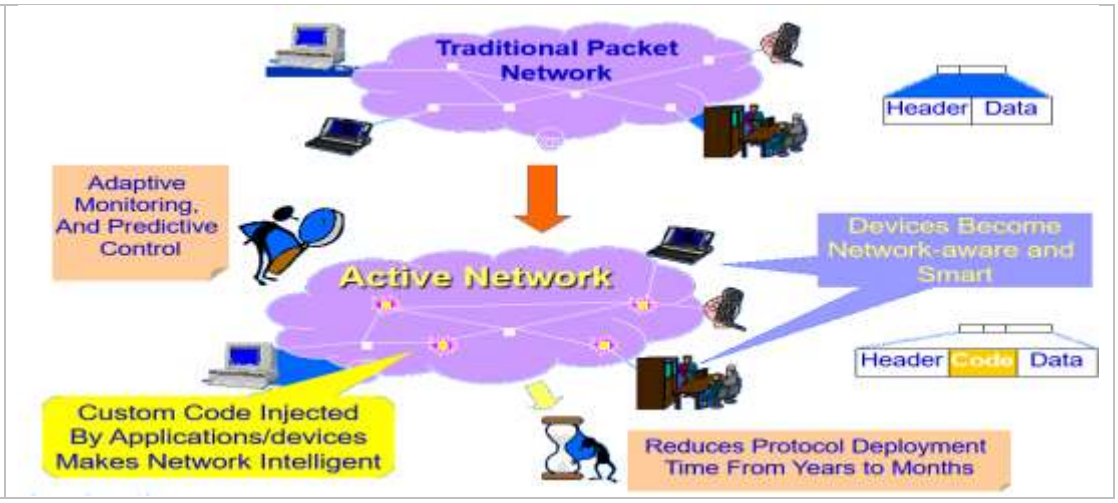
- *Capsules: integrated ANs*
  – Every packet is a program, and carries its code, perhaps in a restricted programming language
  – Programs Integrated into Every Packet Along with Passive Data

Programmable networking has several benefits over traditional networking:

- Reduced long-term costs.
- Ability for applications to maintain information about device capabilities.
- Ability for networks to respond to application status and resource requirements.
- Better allocation of bandwidth and resources.
- Packet prioritization for traffic shaping.
- Improved operational flexibility and enhanced transparency.
- Support for emerging privacy and security technologies.

Evaluation of Active Networks

Active Network can be at least as secured as the legacy/ outdated network. Data and algorithm in an active network are mutable and fluid. It enables more flexible network. It has faster hardware. Devices become network-aware. It also enables faster development of new service.



1.3 Layers, Protocols, Interfaces and Standards

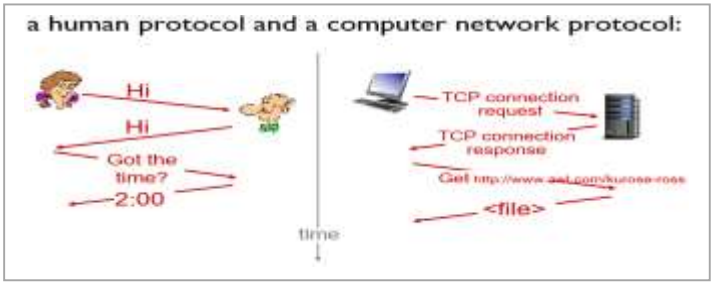
The word protocol comes from the Greek word *protocollon*, meaning a leaf of paper glued to a manuscript volume that describes the contents. Protocols are the formal description of a set of rules and agreements that governor controls and co-ordinate a particular aspect of how devices on a network can communicate. It defines the format, timing, sequencing, and error control mechanisms in data communication. Standard is guidelines that are followed when a new design is to be introduced and actions taken on message transmission, receipt

e.g. *human protocols:*

- ❖ "what's the time?"
- ❖ "I have a question"
- ❖ introductions

… specific message sent
… specific actions taken when message received, or other events
network protocols:

- ❖ machines rather than humans
- ❖ all communication activity in Internet governed by protocols



Protocols control way, in which data communicated, which include the following:

- How the physical network is built
- How computers connect to the network
- How the data is formatted for transmission
- How the data is sent over the network
- How to deal with errors

Standards *: A common set of rules*

Standards Organization : **Standards creation Communities**

***IEEE** (Institute of Electrical and Electronics Engineers) :* IEEE standards affect a wide range of industries including: power and energy,

biomedical and health care, Information Technology (IT), telecommunications, transportation, nanotechnology, information assurance, and many more.

***ANSI** (American National Standards Institute) :* five engineering societies:

- American Institute of Electrical Engineers (AIEE, now IEEE)
- American Society of Mechanical Engineers (ASME)
- American Society of Civil Engineers (ASCE)
- American Institute of Mining Engineers (AIME, now American Institute of Mining, Metallurgical, and Petroleum Engineers)
- American Society for Testing and Materials (now ASTM International)

***ITU** (International Telecommunications Union - formerly CCITT) :* The **International Telecommunication Union** is the specialized agency of the United Nations which is responsible for information and communication technologies (ICT). ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in *assigning satellite orbits, works to improve telecommunication infrastructure in the developing world and establishes worldwide standards.*

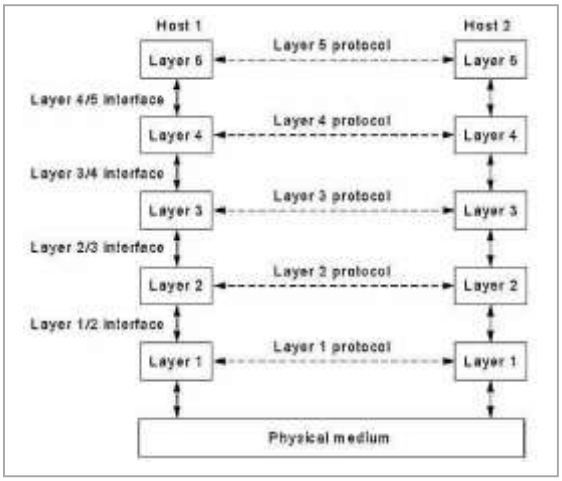
***ISO** (International Organization for Standards) **ISO**,* : is an international standard-setting body composed of representatives from various national standards organizations. The organization circulates worldwide proprietary industrial and commercial standards.

***EIA** (Electronic Industries Association)* : The **Electronic Industries Alliance** (EIA, until 1997 *Electronic Industries Association*) was a standards and trade organization composed as an union of trade associations for electronics manufacturers in the United States.

***ETSI** (European Telecommunications Standards Institute) :*The **European Telecommunications Standards Institute** (**ETSI**) is an independent, non-profit, standardization organization in the telecommunications industry (equipment makers and network operators) in Europe, with worldwide projection. ETSI has been successful in standardizing the Low Power Radio, Short Range Device, GSM cell phone system and the TETRA professional mobile radio system.

***W3C** - World Wide Web Consortium*: W3C also engages in education and outreach, develops software and serves as an open forum for discussion about the Web.

Interfaces-The first computer networks were designed with the *hardware as the main concern and the software as an afterthought.* This strategy no longer works. Network software is now highly structured.



- To reduce their design complexity, most networks are organized as a series or hierarchy of layers or levels.
- The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.
- Layer *n* on one machine communicates with layer *n* on another machine on the network using an some rules known as the layer n protocol. A protocol is an agreement between the communicating parties on how the communication is to proceed.
- The entities comprising the corresponding layers on two communicating machines over the network are called peers.
- Every data and control information is passed from top to the below layer. Additional information including *protocol control information* may be appended by each layer to data as it travels from higher to lower layers in the form of layer headers.

Below layer 1 is the physical medium through which actual communication occur over communication channels.

- Between each pair of adjacent/ together layers there is an interface. The interface defines which primitive operations and services, the lower layer offers to the upper layer. The set of layers and associated protocols is called network architecture.

Protocol

- Special set of rules that end points in a telecommunication connection use when they communicate.
- Specify interactions between the communicating entities.
- Example:
  - Transmission Control Protocol (**TCP**), which uses a set of rules to exchange messages with other Internet points at the information packet level
  - Internet Protocol (**IP**), which uses a set of rules to send and receive messages at the Internet address level
  - Additional protocols that include the Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (**FTP**), each with defined sets of rules to use with corresponding programs elsewhere on the Internet

1.4 Reference Models in Communication Networks : *OSI Reference Model and TCP/IP Reference Model*

layers: each layer implements a service

- via its own internal-layer actions
- relying on services provided by layer below

ISO-OSI Model:

There are many users who use computer network and are located all over the world. To ensure national and worldwide data communication **ISO (International Organization of Standardization.)** developed this model. This is called a model for **Open System Interconnection (OSI)** and is normally called as OSI model. OSI model architecture consists of seven layers. It defines seven layers or levels in a complete communication system.

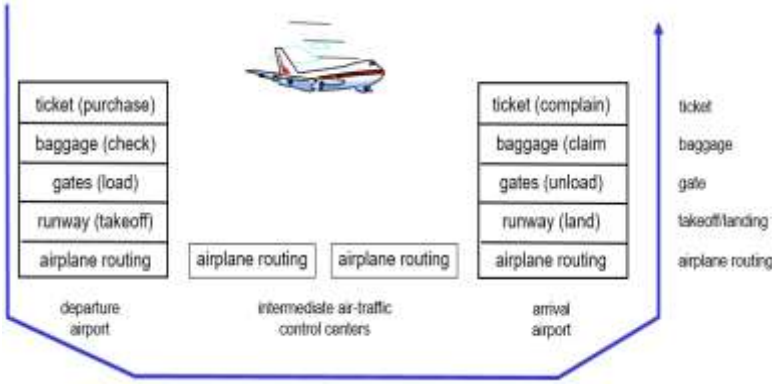


Fig. Layering of airline functionality

Feature of OSI Model :

1. Big picture of communication over network is understandable through this OSI model.
2. We see how hardware and software work together.
3. We can understand new technologies as they are developed.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationships on different networks.

Protocol Data Unit (PDU) :

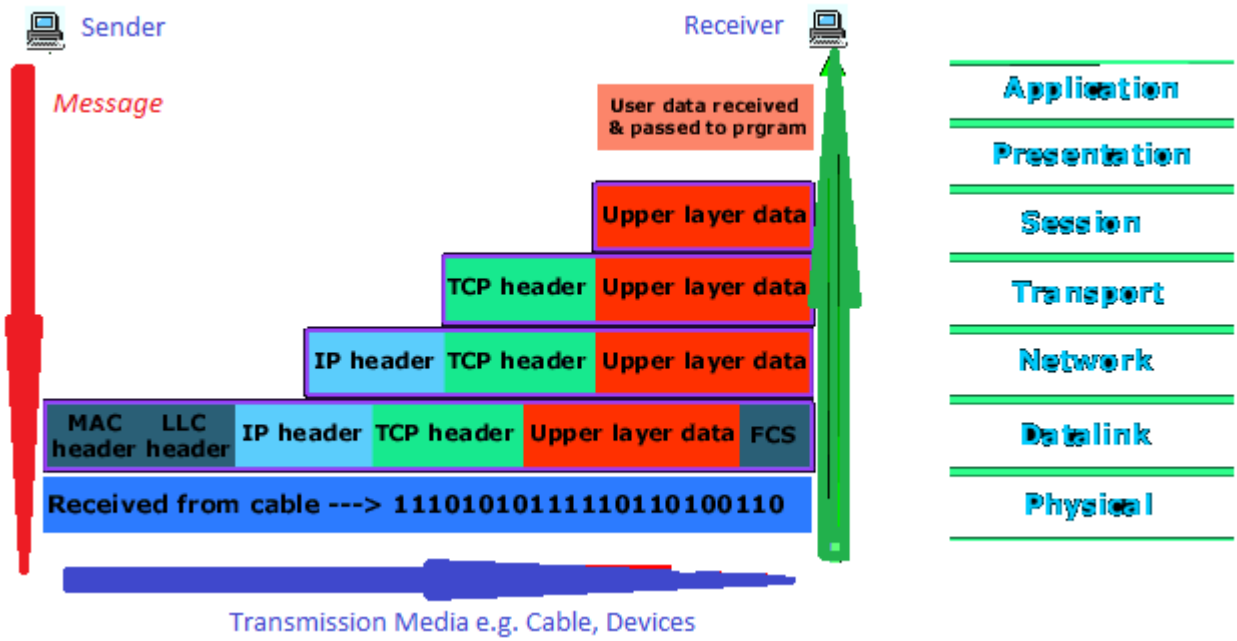
- **In telecommunications Information** that is delivered as a unit among peer entities of a network and that may contain control information, such as address information, or user data, also known as a service data unit (SDU).
- **In a layered system**, a unit of data which is specified in a protocol of a given layer and which consists of protocol-control information and possibly user data of that layer. For example: Bridge PDU or iSCSI PDU

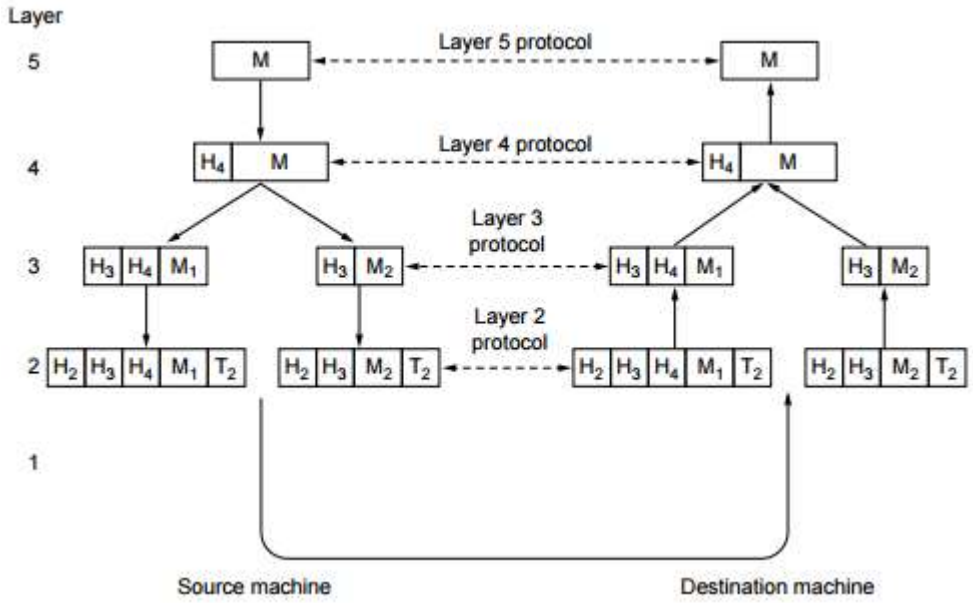
Protocol Control Information(PCI) :

- **In telecommunication**, The queries and replies among communications equipment to determine the respective capabilities of each end of the communications link.
- **For layered systems**, information exchanged between entities of a given layer, via the service provided by the next lower layer, to coordinate their joint operation.

DATA ENCAPSULATION & DECAPSULATION IN THE OSI MODEL

Decapsulation is the process of opening up **encapsulated** data that are usually sent in the form of packets over a communication network. It can be literally defined as the process of opening a capsule, which, in this case, refers to **encapsulated** or wrapped-up data.





Header and Trailer

- Like a web page, header is the upper portion of page and trailer is lower portion of page after main body.
- In data communication, header is the upper part of packet and trailer is lower part of packet which carries the source and destination addresses, synchronization points, information for error detection, etc.
- Is control data added at the beginning and the end of each data unit at each layer of the sender and removed at the corresponding layers of the receiver

Perspective on the OSI Architecture

The annotation along the right-side suggests viewing the seven layers in three parts. The lower three layers contain the logic for a computer to interact with a network. The host is attached physically to the network, uses a data link protocol to reliably communicate with the network, and uses a network protocol to request data exchange with another device on the network and to request network services. Continuing from this perspective, the transport layer provides a reliable end-to-end service regardless of the intervening network facility; in effect, it is the user's liaison to the communications facility. Finally, the upper three layers, taken together, are involved in the exchange of data between end users, making use of a transport service for reliable data transfer.

Another perspective is suggested by the annotation to the left. The lower two layers deal with the link between the host and the network. The next three layers are all involved in transferring data from one host to another: The network layer makes use of the communication network facilities to transfer data from one host to another; the transport layer assures that the transfer is reliable; and the session layer manages the flow of data over the logical connection. Finally, the upper two layers are oriented to the user's concerns, including considerations of the application to be performed and any formatting issues.

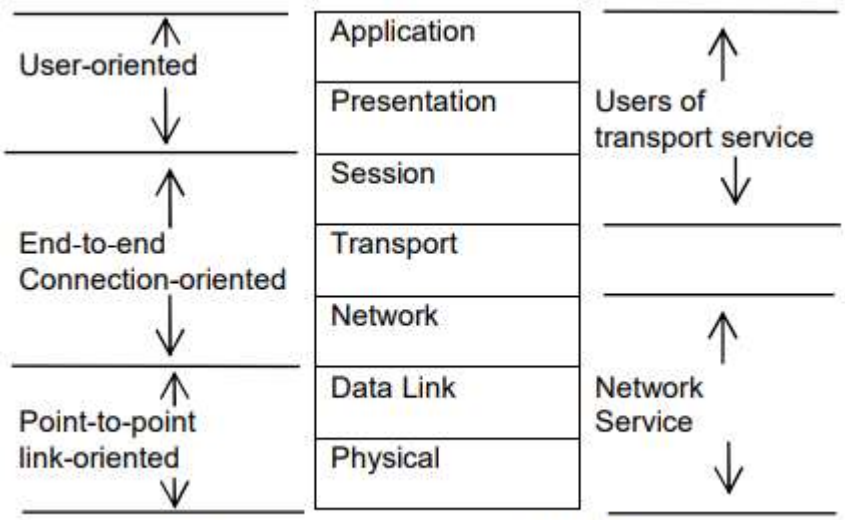


Fig. Perspective on the OSI Architecture.

OSI Seven Layers :-

1.PHYSICAL LAYER

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium e.g Cable-Ethernet, Fibre. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

- Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
  - What signal state represents a binary 1
  - How the receiving station knows when a "bit-time" starts
  - How the receiving station defines a frame
- Physical medium attachment, accommodating various possibilities in the medium:
  - Will an external transceiver (MAU) be used to connect to the medium?
  - How many pins do the connectors have and what is each pin used for?
- Transmission technique: determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signaling.
- Physical medium transmission: transmits bits as electrical or optical signals appropriate for the physical medium, and determines:
  - What physical medium options can be used
  - How many volts/db should be used to represent a given signal state, using a given physical medium

Example :- The data is finally transferred onto the network medium at the Physical layer, in the form of raw bits. Signaling and encoding mechanisms are defined at this layer, as is the hardware that forms the physical connection between the client and the web server

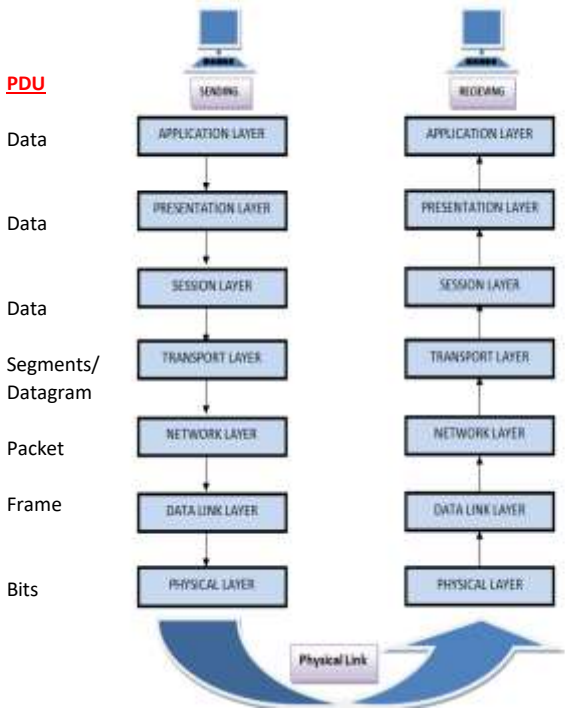


Fig. OSI 7 Layers

OSI model Protocol Suits
7. Application layer NNTP, SIP, SSI, DNS, FTP, Gopher, HTTP, NFS, NTP, SMPP, SMTP, SNMP, Telnet, DHCP, Netconf
6. Presentation layer MIME, XDR
5. Session layer Named pipe, NetBIOS, SAP, PPTP, RTP, SOCKS, SPDY
4. Transport layer TCP, UDP, SCTP, DCCP, SPX
3. Network layer IP , IPv4, IPv6, ICMP, IPsec, IGMP, IPX, AppleTalk, X.25 PLP
2. Data link layer ATM, ARP, IS-IS, SDLC, HDLC, CSLIP, SLIP, GFP, PLIP, IEEE 802.2, LLC, MAC, L2TP, IEEE 802.3, Frame Relay, ITU-T G.hn DLL, PPP, X.25 LAPB, Q.921 LAPD, Q.922 LAPF
1. Physical layer EIA/TIA-232, EIA/TIA-449, ITU-T V-Series, I.430, I.431, PDH, SONET/SDH, PON, OTN, DSL, IEEE 802.3, IEEE 802.11, IEEE 802.15, IEEE 802.16, IEEE 1394, ITU-T G.hn PHY, USB, Bluetooth, RS-232, RS-449,

2.DATA LINK LAYER

The data link layer provides framing and error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. operations package and unpack the data in frames. To do this, the data link layer provides:

- Link establishment and termination: establishes and terminates the logical link between two nodes.
- Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.
- Frame sequencing: transmits/receives frames sequentially.
- Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.
- Frame delimiting: creates and recognizes frame boundaries.
- Frame error checking: checks received frames for integrity.
- Media access management: determines when the node "has the right" to use the physical medium.

Example :- Data cannot be sent directly to a logical address. As packets travel from network to network, IP addresses are translated to hardware addresses, which are a function of the Data-Link layer. The packets are encapsulated into frames to be placed onto the physical medium.

3.NETWORK LAYER

The network layer controls the operation of the subnet, routing : deciding which physical path the data should take based on network conditions, priority of service. Handles packet routing via logical addressing and switching functions. It provides:

- Routing: routes frames among networks.
- Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.

- Frame fragmentation: if it determines that a downstream router's Maximum Transmission Unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
- Logical-physical address mapping: translates logical addresses, or names, into physical addresses

Example **:-** The best path to route the data between the client and the web server is determined by IP, a Network layer protocol. IP is also responsible for the assigned logical addresses on the client and server, and for encapsulating segments into packets.

4.TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers. provides quality of service (QoS) functions and ensures the complete delivery of the data. The integrity of the data is guaranteed at this layer via error correction and similar functions. The transport layer provides:

- Message segmentation*:* accepts a message from the (session) layer above it, **splits** the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station **reassembles** the message.
- Message acknowledgment*:* provides **reliable end-to-end** message delivery with acknowledgments.
- Message traffic control*:* tells the transmitting station to **"back-off"** when no message buffers are available.
- Session multiplexing*:* multiplexes several message streams, or sessions **onto one logical link** and keeps track of which messages belong to which sessions (see session layer).

Example :- HTTP utilizes the TCP Transport layer protocol to ensure the reliable delivery of data. TCP establishes and maintains a connection from the client to the web server, and packages the higher-layer data into segments. A sequence number is assigned to each segment so that data can be reassembled upon arrival.

5.SESSION LAYER or PORT LAYER

Handles authentication and authorization functions. It also manages the connection between the two communicating end points, establishing a connection, maintaining the connection, and ultimately terminating it. The session layer allows session establishment between processes running on different stations. It provides:

- Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.
- Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

For Internet applications, each session is related to a particular port, a number that is associated with a particular upper layer application. For example, the HTTP program or daemon always has port number 80. The port numbers associated with the main Internet applications are referred to as well-known port numbers. Most port numbers, however, are available for dynamic assignment to other applications.

Example :- The Session layer is responsible for establishing, maintaining, and terminating the session between devices, and determining whether the communication is half-duplex or full-duplex. However, the TCP/IP stack generally does not include session-layer protocols, and is reliant on lower-layer protocols to perform these functions.

6.PRESENTATION LAYER

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station. The presentation layer provides:

- Character code translation: for example, ASCII to EBCDIC.
- Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
- Data compression: reduces the number of bits that need to be transmitted on the network.
- Data encryption: encrypt data for security purposes. For example, password encryption.**7.APPLICATION LAYER** The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:
  - Resource sharing and device redirection
  - Remote file access, printer access
  - Inter-process communication
  - Network management
  - Directory services
  - Electronic messaging (such as mail)
  - Network virtual terminals

Example : The Internet can provide data in a wide variety of formats, a function of the Presentation layer. Common formats on the Internet include HTML, XML, PHP, GIF, and JPEG. Any encryption or compression mechanisms used on a website are also considered a Presentation layer function.

7.Application Layer

Application layer is the top most layer, which are involved in communication system, in which initiated and reflects because this layer is on the top of the layer stack, it does not serve any other layers.

The application layer is not the application itself that is doing the communication. It is a service layer that provides these services:

- Simple Mail Transfer Protocol, Email clients
- File transfer
- Web surfing, Web chat
- Network data sharing
- Virtual terminals

Example :- The web browser serves as the user interface for accessing a website. The browser itself does not function at the Application layer. Instead, the web browser invokes the Hyper Text Transfer Protocol (HTTP) to interface with the remote web server, which is why http:// precedes every web address.

TCP/IP REFERENCE Model

TCP/IP protocols map to a four-layer conceptual model known as the ***DARPA model*** , named after the U.S. government agency that initially developed TCP/IP. The four layers of the DARPA model are: Application, Transport, Internet, and Network Interface. Each layer in the DARPA model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) model.

IP is the clerk *- deals with addressing of packets like mapping the logical/network address to MAC address.*

TCP is the postman *which deals with delivering the data packets to various hosts over the internet. It is dependent on the IP. Provides services like Flow control , error detection and correction.*

TCP/IP is transmission control protocol and internet protocol. Protocols are set of rules which govern every possible communication over the internet. These protocols describe the movement of data between the host computers or internet and offers simple naming and addressing schemes.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact until the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

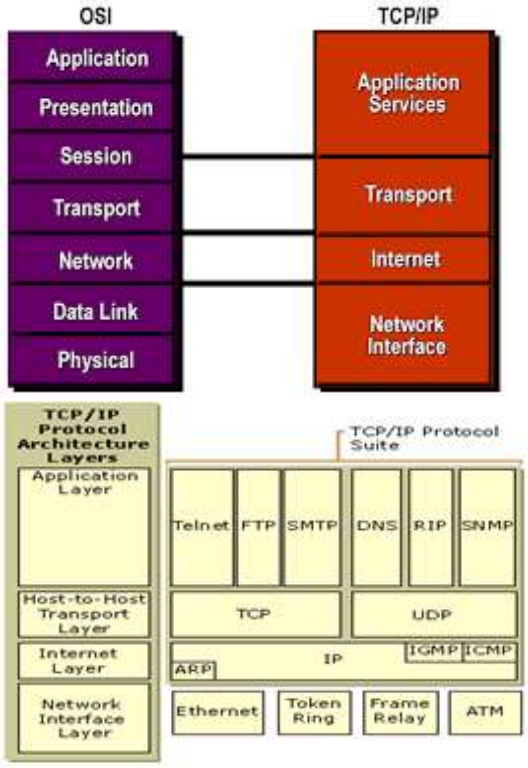


Fig. TCP/IP Protocol Architecture

TCP/IP protocol suite

Application layer

BGP, DHCP, DNS, FTP, HTTP, IMAP, LDAP, MGCP, NNTP, NTP, POP, ONC/RPC, RTP, RTSP, RIP, SIP, SMTP, SNMP, SSH, Telnet, TLS/SSL, XMPP

Transport layer

TCP, UDP, DCCP, SCTP, RSVP

Internet layer

IP , IPv4, IPv6, ICMP, ICMPv6, ECN, IGMP, IPsec

Link layer

ARP, NDP, OSPF, Tunnels , L2TP, PPP, MAC , Ethernet, DSL, ISDN, FDDI,

1.Network Interface Layer : Deals with all physical components of network connectivity between the network and the IP protocol.

The *Network Interface layer* (also called the Network Access layer) is responsible for placing TCP/IP packets on the network medium and receiving TCP/IP packets off the network medium. TCP/IP was designed to be independent of the network access method, frame format, and medium. In this way, TCP/IP can be used to connect differing network types. These include LAN technologies such as Ethernet and Token Ring and WAN technologies such as X.25 and Frame Relay. Independence from any specific network technology gives TCP/IP the ability to be adapted to new technologies such as Asynchronous Transfer Mode (ATM).

The Network Interface layer encompasses the Data Link and Physical layers of the OSI model.

2.Internet Layer : Contains all functionality that manages the movement of data between two network devices over a routed network. The *Internet layer* is responsible for addressing, packaging, and routing functions. The core protocols of the Internet layer are IP, ARP, ICMP, and IGMP.

- The *Internet Protocol* (**IP**) is a routable protocol responsible for IP addressing, routing, and the fragmentation and reassembly of packets.
- The *Address Resolution Protocol* (**ARP**) is responsible for the resolution of the Internet layer address to the Network Interface layer address such as a hardware address.
- The *Internet Control Message Protocol* (**ICMP**) is responsible for providing diagnostic functions and reporting errors due to the unsuccessful delivery of IP packets.

- The *Internet Group Management Protocol* (**IGMP**) is responsible for the management of IP multicast groups.

The Internet layer is analogous to the Network layer of the OSI model.

3.Transport Layer (Host-to-Host): Manages the flow of traffic between two hosts or devices, ensuring that data arrives at the application on the host for which it is targeted. The *Transport layer* (also known as the Host-to-Host Transport layer) is responsible for providing the Application layer with session and datagram communication services. The core protocols of the Transport layer are *Transmission Control Protocol* (TCP) and the *User Datagram Protocol* (UDP).

- **TCP** provides a one-to-one, connection-oriented, reliable communications service. TCP is responsible for the establishment of a TCP connection, the sequencing and acknowledgment of packets sent, and the recovery of packets lost during transmission.
- **UDP** provides a one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small (such as the data that would fit into a single packet), when the overhead of establishing a TCP connection is not desired or when the applications or upper layer protocols provide reliable delivery.

The Transport layer encompasses the responsibilities of the OSI Transport layer and some of the responsibilities of the OSI Session layer.

4.Application Layer : Acts as final endpoints at either end of a communication session between two network hosts(Sender, Receiver). The *Application layer* provides applications the ability to access the services of the other layers and defines the protocols that applications use to exchange data. There are many Application layer protocols and new protocols are always being developed.

The most widely-known Application layer protocols are those used for the exchange of user information:

- The Hypertext Transfer Protocol (**HTTP**) is used to transfer files that make up the Web pages of the World Wide Web.
- The File Transfer Protocol (**FTP**) is used for interactive file transfer.
- The Simple Mail Transfer Protocol (**SMTP**) is used for the transfer of mail messages and attachments.
- Telnet, a terminal emulation protocol, is used for logging on remotely to network hosts.

Additionally, the following Application layer protocols help facilitate the use and management of TCP/IP networks:

- The Domain Name System (**DNS**) is used to resolve a host name to an IP address.
- The Routing Information Protocol (**RIP**) is a routing protocol that routers use to exchange routing information on an IP internetwork.
- The Simple Network Management Protocol (**SNMP**) is used between a network management console and network devices (routers, bridges, intelligent hubs) to collect and exchange network management information.

1.5 Comparison of OSI and TCP/ IP model

OSI (Open System Interconnection)	**TCP/IP(Transmission Control Protocol / Internet Protocol)**
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.
6. Network layer of OSI model provides both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.
7. OSI model has a problem of fitting the protocols into the model.	7. TCP/IP model does not fit any protocol
8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	9. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
10. It has 7 layers	10. It has 4 layers
11. Layer was first developed than protocol	11. Protocol were first developed than layer

1.6 Example Network

*** The Internet or WWW:** The **Internet** is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide. It is a *network of networks* that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and peer-to-peer networks for file sharing.

Internet Users by Country (2016) *:* 1.China, 2.India, 3.USA, 4.Brazil, 5.Japan,……., 70.Nepal,….,200. Marshall Islands

Sources : http://www.internetlivestats.com/internet-users-by-country/

Regional Internet Registries (RIRs) allocate IP addresses:

- African Network Information Center (AfriNIC) for Africa
- American Registry for Internet Numbers (ARIN) for North America
- Asia-Pacific Network Information Centre (APNIC) for Asia and the Pacific region
- Latin American and Caribbean Internet Addresses Registry (LACNIC) for Latin America and the Caribbean region
- Réseaux IP Européens – Network Coordination Centre (RIPE NCC) for Europe, the Middle East, and Central Asia

The Internet carries many network services, most prominently mobile apps such as social media apps, the World Wide Web, electronic mail, multiplayer online games, Internet telephony, and file sharing services

The Internet has enabled new forms of social interaction, activities, and social associations. This phenomenon has given rise to the scholarly study of the sociology of the Internet.e.g. Telecomuting, Crowd Sourcing, Social Medias)

Internet resources, hardware, and software components are the target of malicious attempts to gain unauthorized control to cause interruptions or access private information. Such attempts include computer viruses which copy with the help of humans, computer worms which copy themselves automatically, denial of service attacks, ransomware, botnets, and spyware that reports on the activity and typing of users. Usually, these activities constitute cybercrime. Defense theorists have also speculated about the possibilities ofcyber warfare using similar methods on a large scale

* X.25 : WAN technology

X.25 was designed for transmitting analog data such as voice conversations.

The X.25 specification defines only the interface between a subscriber (**Data Terminal Equipment-DTE**) and an X.25 network (**Data Circuit terminal Equipment-DCE**). **X.25** defines the interface between two X.25 networks to allow connections to traverse two or more networks. X.25 does not specify how the network operates internally – many X.25 network implementations used something very similar to X.25 or X.75 internally, but o thers used quite different protocols internally. The ISO equivalent protocol to X.25, ISO 8208, is compatible with X.25, but additionally includes provision for two X.25 DTEs to be directly connected to each other with no network in between.

-*X.25* is a standard suite of protocols used for packet switching across computer networks. The X.25 protocols works at the physical, data link, and network layers (Layers 1 to 3) of the OSI model.

- **Physical layer**: This layer specifies the physical, electrical, functional and procedural characteristics to control the physical link between a DTE and a DCE. Common implementations use X.21, EIA-232, EIA-449 or other serial protocols.
- **Data link layer**: The data link layer consists of the link access procedure for data interchange on the link between a DTE and a DCE. In its implementation, the Link Access Procedure, Balanced (LAPB) is a data link protocol that manages a communication session and controls the packet framing. It is a bit-oriented protocol that provides error correction and orderly delivery.
- **Packet layer**: This layer defined a packet-layer protocol for exchanging control and user data packets to form a packet-switching network based on virtual calls, according to the Packet Layer Protocol.

-Each X.25 packets contains up to 128 bytes of data. The X.25 network handles packet assembly at the source device, delivery, and then dis-assembly at the destination. X.25 packet delivery technology includes not only switching and network-layer routing, but also error checking and re-transmission logic should delivery failures occur.

-X.25 supports multiple simultaneous conversations by multiplexing packets and using virtual communication channels.

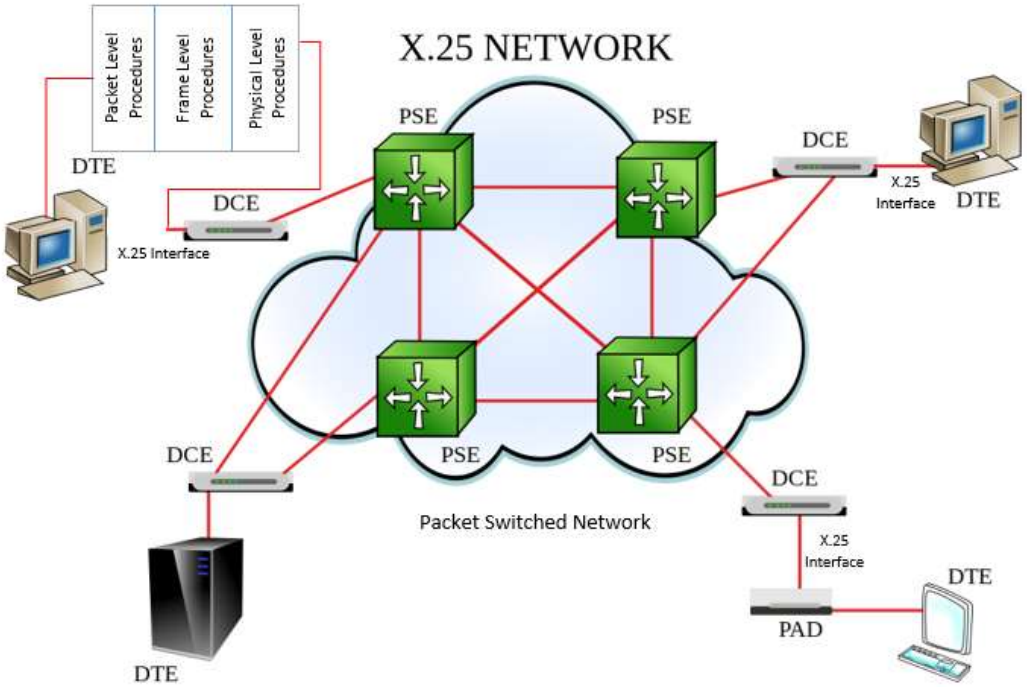
-X.25 was originally designed more than 25 years ago to carry voice over analog telephone lines (dialup networks). Typical applications of X.25 today include automatic teller machine networks and credit card verification networks. X.25 also supports a variety of mainframe terminal/server applications.

- With the widespread acceptance of Internet Protocol (IP) as a standard for corporate networks, many X.25 applications are now being migrated to cheaper solutions using IP as the network layer protocol and replacing the lower layers of X.25 with Ethernet or ATM hardware.

History of X.25

X.25 was originally developed in the 1970s to carry voice over analog telephone lines—dial-up networks. Typical applications of X.25 included automatic teller machine networks and credit card verification networks.

In the early 90s, many X.25 networks were replaced by Frame Relay in the U.S. Many older public networks outside the U.S. continued to use X.25 until just recently. Most networks that once required X.25 now use the less complex Internet Protocol. X-25 is still used in some ATMs and credit card verification networks.



- **DTE** (Data Terminal Equipment): An end user equipment that converts user information into signals or reconverts received signals. E.g. terminals, computer, protocol converters, multiplexors
- **DCE** (Data Communication Equipment): data communication devices located between DTE e.g. MODEM, NIC Cards
- **PSE** (Packet Switching Exchange): breaks data in to packets.
- **PAD** (Packet Assembly/ Disassembly): a device used to enable DTE, not equipped for packet switching to access a packet-switched network

Advantages of X.25

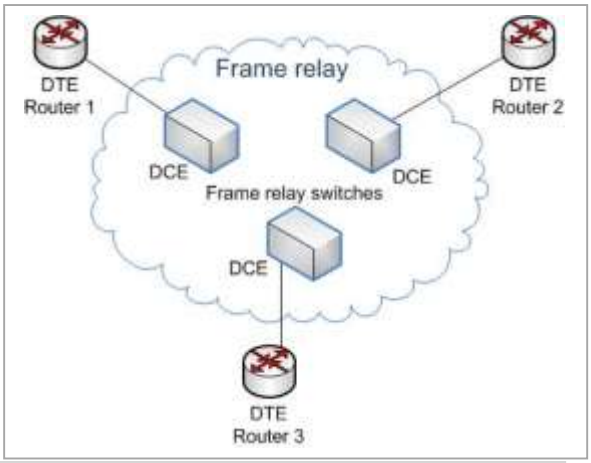
- Works well in noisy transmission mediums (More errors and Packet drops)
- It is one of the oldest WAN technology (Helps in development of technology research)
- Used for terminal and time-sharing connection
- Helps in data communication especially of packet switched networks
- The data link layer is designed for error detection and corrections
- The network layer protocol performs the addressing, flow control, delivery confirmation

Dis-advantages of X.25

- Since it was initially developed for private use not the internet, it could not meet public demands needs.
- Double overhead X.25 and the internet have their own network layer
- Disappointed with X.25, some organizations started their own private WAN by leasing T-1(max. 1.544 Mbps) or T3(44.736 Mbps)
- Not simplified compared to Frame Relay
- Could not handle bursty data or a continuous transfer of data without interruption (Bandwidth on demand)

* Frame Relay: Layer 2 WAN Technology

Frame Relay is a standardized wide area network technology that specifies the physical and data link layers of digital telecommunications channels using a packet switching methodology. Originally designed for transport across Integrated Services Digital Network (ISDN) infrastructure, it may be used today in the context of many other network interfaces.



Network providers commonly implement Frame Relay for Voice (VoFR) and data as an encapsulation technique used between local area networks (LANs) over a wide area network (WAN). Each end-user gets a private line (or leased line) to a Frame Relay node. The Frame Relay network handles the transmission over a frequently changing path transparent to all end-user extensively used WAN protocols. It is less expensive than leased lines and that is one reason for its popularity. The extreme

simplicity of configuring user equipment in a Frame Relay network offers another reason for Frame Relay's popularity.

With the advent of Ethernet over fiber optics, MPLS, VPN and dedicated broadband services such as cable modem and DSL, the end may loom for the Frame Relay protocol and encapsulation. However, many rural areas remain lacking DSL and cable modem services. In such cases, the least expensive type of non-dial-up connection remains a 64-kbit/s Frame Relay line. Thus, a retail chain, for instance, may use Frame Relay for connecting rural stores into their corporate WAN.

The designers of Frame Relay aimed to provide a telecommunication service for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between end-points in a wide area network (WAN). Frame Relay puts data in variable-size units called "frames" and leaves any necessary error-correction (such as retransmission of data) up to the end-points. This speeds up overall data transmission. For most services, the network provides a permanent virtual circuit (PVC), which means that the customer sees a continuous, dedicated connection without having to pay for a full-time leased line, while the service-provider figures out the route each frame travels to its destination and can charge based on usage.

Analogy: The collection of bits within a structure is called a frame. When it arrives at a switching point it is relayed from one interface to another and in that process the DLCI (Data Link Connection Idenfier) is switched. Imagine a relay race. The runner passes the stick to the next runner. The stick (data) does not change but the runner (DLCI) does. The advantage of a frame is that you only align your clocks for the duration of the frame whereas with asynchronous you have to align your clock for each character / byte.

How FR Works?

- The DTE (router) sends frames to the DCE (Frame relay Switches) on the WAN edge
- The frames moves from switch to switch across the WAN to the destination DCE (frame relay switch) on the WAN edge
- The destination DCE delivers the frames to the destination DTE

Advantages of FR

- Cost Savings: FR offers reduction of physical local loops over private line network as frame uses a virtual circuit for each new connection
- Higher circuit utilization: FR makes use of physical circuit by statistically multiplexing multiple PVCs over a single physical circuit
- Higher network availability: FR network employs switches that support automatic routing of PVC around circuit failure
- Extended Technology Life Duration: FR is backwards compatible with older technologies like X.25 and forward compatible with newer technologies like ATM and MPLs
- Protocol Independence: Supports wide variety of application transports and meets the throughput requirements.
- Performance: FR services offers higher speed with lower delay as compared to X.25

Disadvantages of FR

- T-3(44.736 Mbps) data rate is not enough for protocols with higher data rates
  Note: T-3 leased line is used for longer distance, higher bandwidth than T1; both are used for digital data transmission system used in telecommunications
- Allows variable length frames
- Create varying delays for different users
- Not suitable for sending delay sensitive data such as real; time voice or video or teleconferencing.

Comparison between FR and X.25

Attributes	Frame Relay	X.25
Error Detection	No	Yes, hence it provides error free delivery. It contains fields which are used for error and flow control.
Layers	It has Physical layer and data link layer. Hence higher performance and greater transmission rate is achieved.	It has physical, data link and network layers.
PDU	It prepares and sends frames.	It prepares and sends packets.
BW allicattion	It can dynamically allocate bandwidth.	Fixed bandwidth is available in X.25 network.
Typical Speed (bandwidth)	High (No error detection)	Low
LAN connectivity for fast file transfers	Suitable	Not Suitable
Protocol Overhead, Complexity	Minimal	High
Voice support	Good	Poor

***Ethernet :** LAN technology

In 1973, Robert Metcalfe from New York devised a system of joining multiple endpoint devices on a network, and drew it out as a memo (pictured above). The nowhere-in-particular field between the controller and the endpoints he referred to as "*The Ether*". The resulting network was then called *the Ethernet*.

Ethernet is a type of network cabling and signaling specifications developed by **Xerox** in the late 1970. While Internet is a global network, Ethernet is a local area network (LAN). No computer should be an island. With Ethernet, file sharing and printer sharing among machines became possible. The term "ether" was coined by Greek philosopher Aristotle to describe the "divine element" in the heaven. In the 17th century, French philosopher and mathematician Rene Descartes theorized that the universe has no void; all space, including the heaven and the earth, is filled with ether, which is composed of very fine particles. In short, "ether" is said to be a kind of substance that exists everywhere. Although this is a misconception, network developers still adopted the term "ether" and therefore "Ethernet" means "a network of everywhere."

Ethernet uses a communication concept called datagrams to get messages across the network. The Ethernet datagrams take the form of self-contained packets of information. These packages have fields containing information about the data, their origin, their destination and the type of data. The data field in each package can contain up to 1500 bytes. Take mailing as a metaphor. An Ethernet package is not just a letter. It is also provided with the sender address, the receiver address, the stamp indicating what the package's contents are.

There are several standards of Ethernet, such as **1000BaseT**, 10GBaseT...etc. The number stands for signaling speed: "**1000**" is 1000 mega bit per second. However, it is important to point out that this number indicates the "ideal" situation. The actual speed might be slower. "**Base**" means Baseband, which uses a single carrier frequency so that all devices connected to the network can hear all transmissions. **"T"** stands for twisted pair cable.

Ethernet suffers from collision when it is running in half-duplex mode. What is half-duplex? CB radio is a typical example of half-duplex. When using a CB radio, you can either send a message or receive a message at one time. When two or more computers attempt to send data at the same time, a collision occurs. Nevertheless, switches make it possible to run Ethernet in full-duplex mode. In this mode, two computers establish a point-to-point connection in full-duplex and thus collisions are avoided.

Types of Ethernet Cable

i. Fast Ethernet : *100 Mbit/s, Cat-5*

Fast Ethernet refers to an Ethernet network that can transfer data at a rate of 100 Mbit/s. It can be based on a twisted pair or fiber optic cable. (The older 10 Mbit/s Ethernet is still installed and used, but such networks do not provide the necessary bandwidth for some network video applications.)

Most devices that are connected to a network, such as a laptop or a network camera, are equipped with a 100BASE-TX/10BASE-T Ethernet interface, most commonly called a 10/100 interface, which supports both 10 Mbit/s and Fast Ethernet. The type of twisted pair cable that supports Fast Ethernet is called a Cat-5 cable.

ii. Gigabit Ethernet : *1,000 Mbit/s (1 Gbit/s), Cat-5e*

Gigabit Ethernet, which can also be based on a twisted pair or fiber optic cable, delivers a data rate of 1,000 Mbit/s (1 Gbit/s) and is becoming very popular. It is expected to soon replace Fast Ethernet as the de facto standard.

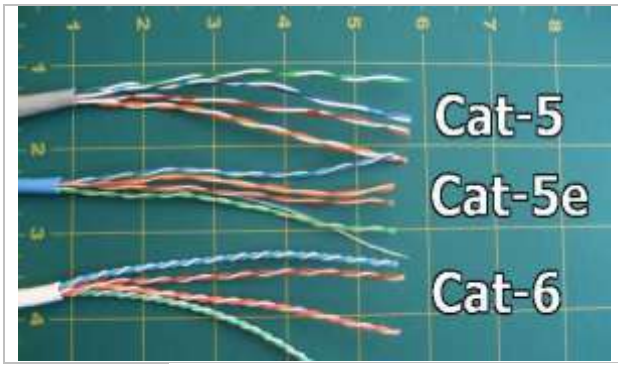
- The type of twisted pair cable that supports Gigabit Ethernet is a Cat-5e cable, where all four pairs of twisted wires in the cable are used to achieve the high data rates. Cat-5e or higher cable categories are recommended for network video systems. Most interfaces are backwards compatible with 10 and 100 Mbit/s Ethernet and are commonly called 10/100/1000 interfaces.
- For transmission over longer distances, fiber cables such as 1000BASE-SX (up to 550 m/1,639 ft.) and 1000BASE-LX (up to 550 m with multimode optical fibers and 5,000 m with single-mode fibers) can be used.

iii. 10 Gigabit Ethernet : *10 Gbit/s (10,000 Mbit/s), Cat-6a or Cat-7*

10 Gigabit Ethernet is the latest generation and delivers a data rate of 10 Gbit/s (10,000 Mbit/s), and a fiber optic or twisted pair cable can be used. 10GBASE-LX4, 10GBASE-ER and 10GBASE-SR based on an optical fiber cable can be used to bridge distances of up to 10,000 m (6.2 miles). With a twisted pair solution, a very high quality cable (Cat-6a or Cat-7) is required. 10 Gbit/s Ethernet is mainly used for backbones in high-end applications that require high data rates.

The Major Categories of Ethernet Cables

There are two main physical differences between Cat-5 and Cat-6 cables, the number of twists per cm in the wire, and sheath thickness.



Category	*Cable Type*	*Max. Data Trans Speed*	*Max Bandwidth*
Cat 3	UTP	10 Mbps	16 MHz
Cat 5	UTP	10/100 Mbps	100 MHz
Cat 5 e	UTP	1000 Mbps	100 MHz
Cat 6	UTP or STP	1000 Mbps	250 MHz
Cat 6 a	STP	10,000 Mbps	500 MHz
Cat 7	SSTP	10,000 Mbps	600 MHz

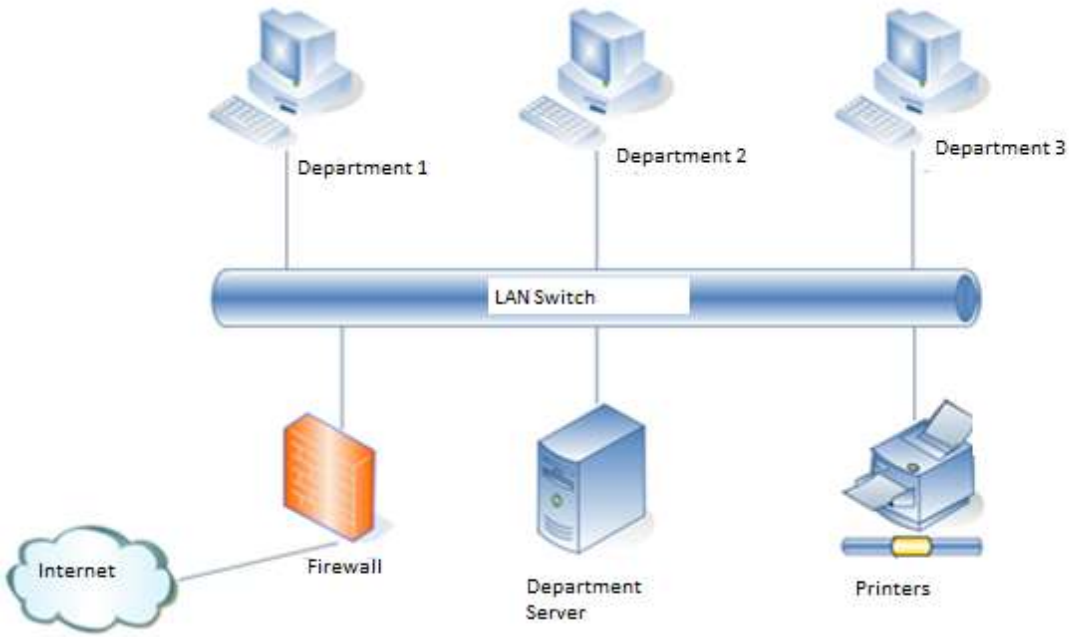


Fig. Ethernet LAN Diagram

*xDSL (*Digital Subscriber Lines*): MAN Technology

Digital subscriber line (**DSL**; originally **digital subscriber loop**) is a family of technologies that are used to transmit digital data over telephone lines. In telecommunications marketing, ADSL is the most commonly installed DSL technology, for Internet access. DSL service can be delivered simultaneously with wired telephone service on the same telephone line. This is possible because DSL uses higher frequency bands for data. On the customer premises, a DSL filter on each non-DSL outlet blocks any high-frequency interference to enable simultaneous use of the voice and DSL services.

DSL technologies use sophisticated modulation schemes to pack data onto copper wires. They are sometimes referred to as last-mile technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations.

xDSL is similar to ISDN in as much as both operate over existing copper telephone lines (POTS – Plain Old Telephone Service – home uses) and both require the short runs to a central telephone office (usually less than 20,000 feet). However, xDSL offers much higher speeds - up to 32Mbps for upstream traffic, and from 32 Kbps to over 1 Mbps for downstream traffic.

A **DSLAM** (Digital Subscriber Line Access Multiplexer) is a network device, usually at a telephone company central office, that receives signals from multiple customer Digital Subscriber Line (DSL) connections and puts the signals on a high-speed backbone line using multiplexing techniques.

Types of xDSL

i. Asynchronous/Asymmetric-DSL(**ADSL**): broadband communications technology used for connecting to the Internet. Provides more bandwidth for downstream than upstream.
ii. Synchronous/Symmetric-DSL(**SDSL**). : allows more data to be sent over existing copper telephone lines (POTS). Provides equal bandwidth for upstream and downstram.
iii. *High-data-rate DSL (**HDSL**)*: requires multiple telephone lines.
iv. *Very high DSL (**VDSL**)*: Fastest DSL service.

DSL Type	Max. Send Speed	Max. Receive Speed	Max. Distance	Lines Required	Phone Support
ADSL	800 Kbps	8 Mbps	18,000 ft (5,500 m)	1	Yes
HDSL	1.54 Mbps	1.54 Mbps	12,000 ft (3,650 m)	2	No
SDSL	2.3 Mbps	2.3 Mbps	22,000 ft (6,700 m)	1	No
VDSL	16 Mbps	52 Mbps	4,000 ft (1,200 m)	1	Yes

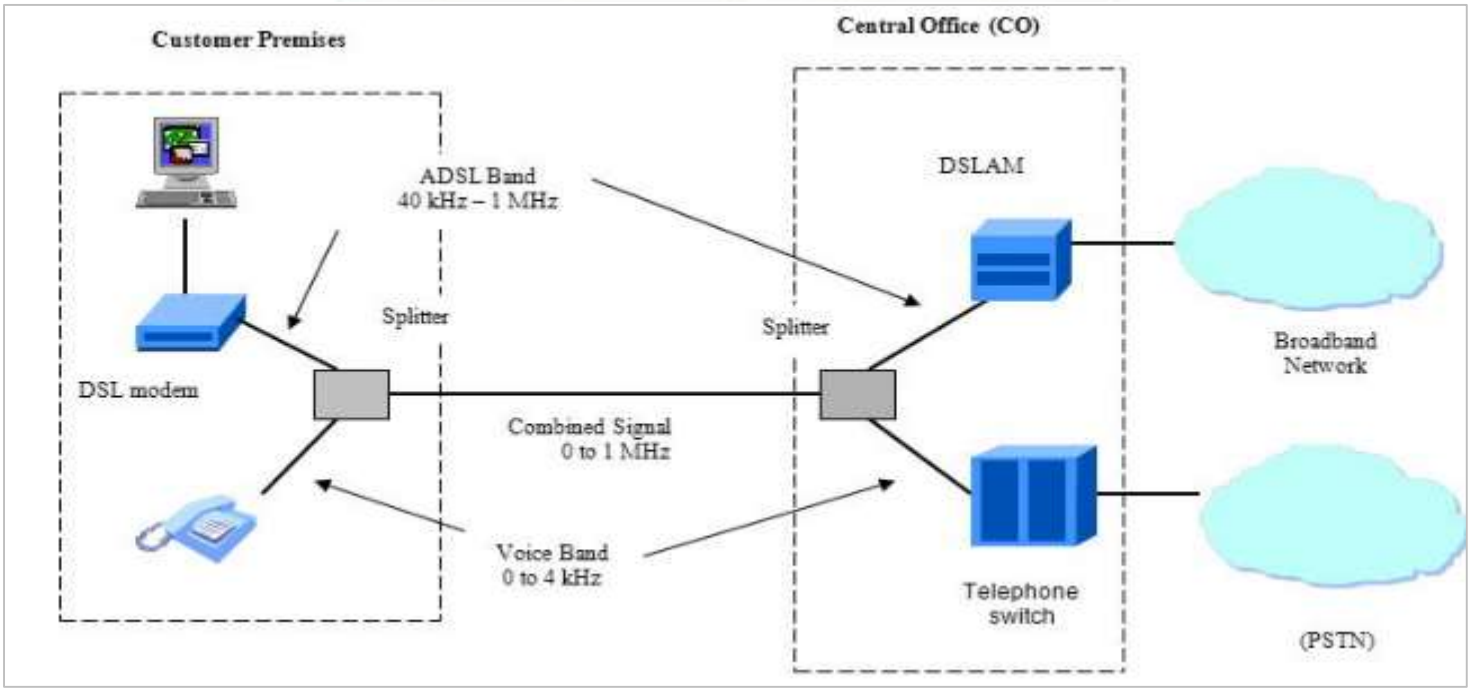


Fig. DSL Architecture

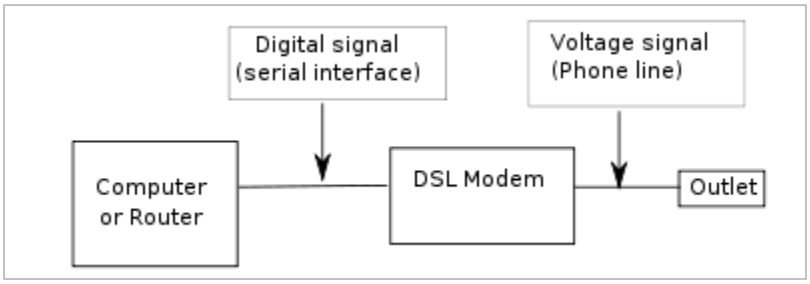


Fig. DSL Modem schematic

***** VoIP (Voice over Internet Protocol)

VoIP or IP telephony is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, i.e. intranet, Internet. The terms Internet telephony, broadband telephony, and broadband phone service specifically refer to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the public switched telephone network (PSTN).

These protocols can be used by special-purpose software, such as Jitsi, or integrated into a web page (web-based VoIP), like Google Talk.

How does VOIP work?

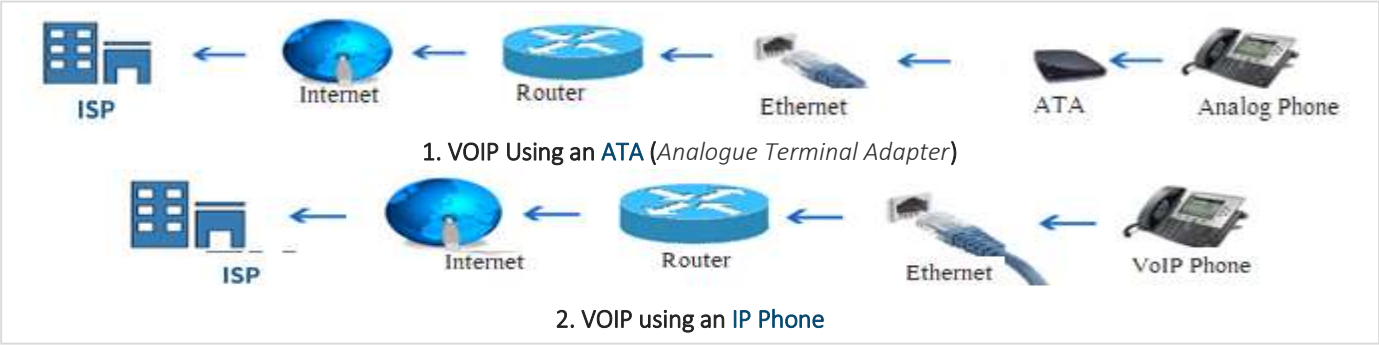
A way is required to turn analog phone signals into digital signals that can be sent over the Internet. This function can either be included into the phone itself or in a separate box like an ATA .

1. VOIP Using an ATA (*Analogue Terminal Adapter*)

… Ordinary Phone ---- ATA ---- Ethernet ---- Router ---- Internet ---- VOIP Service Provider

2. VOIP using an IP Phone

… IP Phone ----- Ethernet ----- Router ---- Internet ---- VOIP Service Provider



1. VOIP Using an ATA (*Analogue Terminal Adapter*)

2. VOIP using an IP Phone

Methods of VoIP Configurations

I. **PC – to – PC** : Call transfer between PC
II. **PC – to – Hardphone** : Call transfer between PC and Hardphone
III. **Hardphone – to – Hardphone** : Call transfer between Hardphone

VoIP is crime : if we are used VoIP technology with out permission from ISP or Government or Tax Cheating

*** NGN and MPLS(**Next Generation Network and Multiprotocol Label Switching)

- Today, telephony, the internet, and the cellular mobile networks continue to be different domains, each has its own protocols and services.
- The general idea behind the NGN is that one network transports all type of data and provides services (voice, data, and all sorts of media e.g. video) by encapsulating the into packets, similar to those used on the internet.
- NGN are commonly built around the IP and therefore the term all IP is also sometimes used to describe the transformation toward NGN.
- Todays networks are divided into :
  - The Public Switched Telephone Network (e.g. telephone)
  - The Packet Switched Network (e.g. Internet)
  - The Mobile Networks (e.g. cellular)

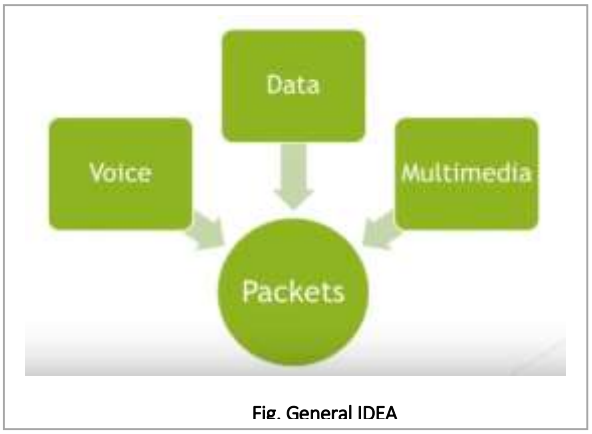


Fig. General IDEA

A Next Generation Network (NGN) is a packet-based network able to provide services including Telecommunication Services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access by users to different service providers. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

A Next Generation Networks (**NGN**) is a packet-based network able to provide Telecommunication Services to users and able to make use of multiple broadbands, QoS-enabled *transport technologies and in which service-related functions* are independent of the underlying transport-related technologies.

NGN is a different concept from Future Internet, which is more focused on the evolution of Internet in terms of the variety and interactions of services offered.

From a practical perspective, NGN involves three **main architectural changes** that need to be looked at separately:

- In the core network, NGN implies a merging of several (dedicated or overlay) transport networks each historically built for a different service into one core transport network (often based on IP and Ethernet). It implies amongst others the migration of voice from a circuit-switched architecture (PSTN) to VoIP, and also migration of legacy services such as X.25, frame relay (either commercial migration of the customer to a new service like IP VPN, or technical emigration by emulation of the "legacy service" on the NGN).
- In the wired access network, NGN implies the migration from the dual system of legacy voice next to xDSL setup in local exchanges to a converged setup in which the DSLAMs(digital subscriber line access multiplexer) integrate *voice ports* or VoIP, making it possible to remove the voice switching infrastructure from the exchange.
- In the cable access network, NGN convergence implies migration of constant bit rate voice to Cable Labs/ Packet Cable standards that provide VoIP and SIP services.

Characteristics of NGN:

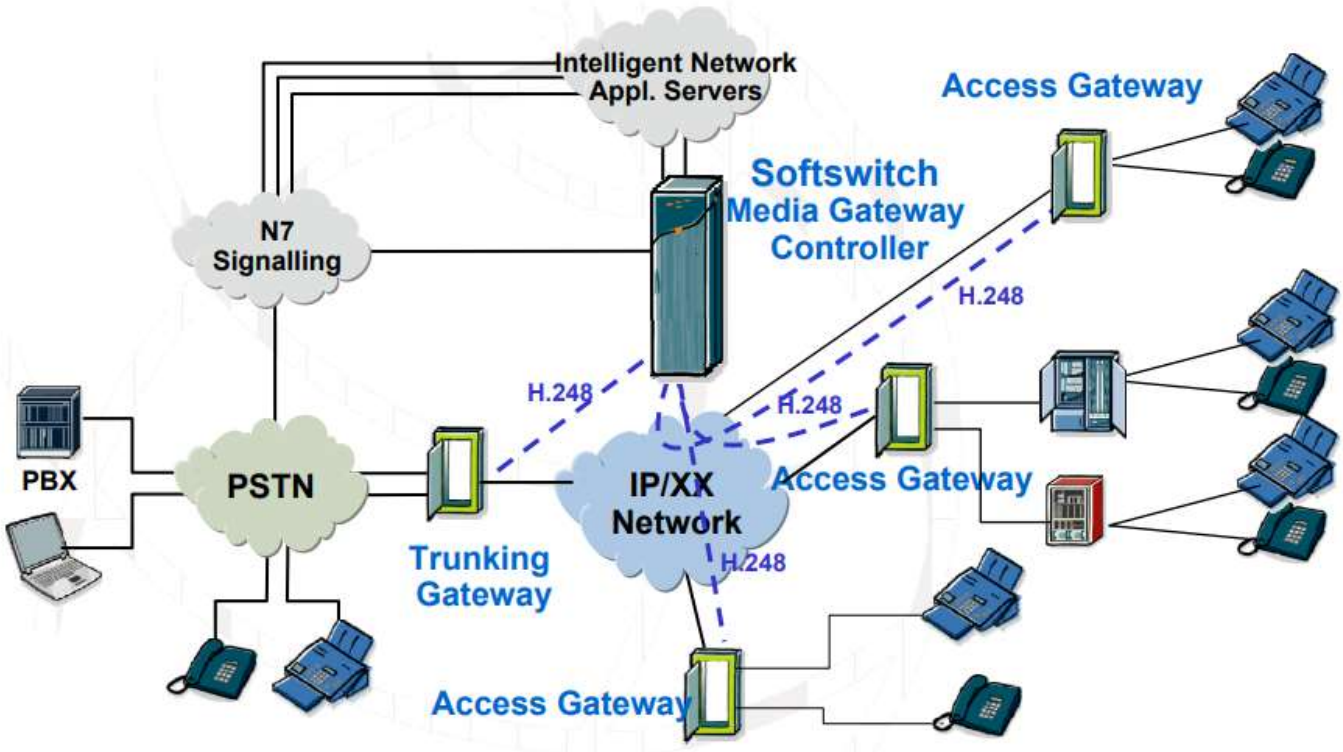
- Unified Global Network Platform : Support for a wide range of services, applications and mechanisms based on service building blocks (including real time/ streaming/ non-real time services and multi-media)
- Packet Based Network
- Provides Telecommunication Services to Users
- QoS – Enabled Transport Technology

- Generalized mobility
- Converged services between Fixed/Mobile

NGN Services or Applications

i. **Voice Telephony**: Call waiting, forwarding, 3-way calling
ii. **Voice Portal**: provides callers with anywhere anytime access to information like news, weather, account balance using simple voice commands and any telephone
iii. **Data Services**: bandwidth-on-demand, connection reliable
iv. **Multimedia services**: displaying visual information e.g. real-time streaming
v. **Public Network Computing**: provides public network-based computing services for business and customers
vi. **E-Commerce**: allows customers to purchase goods and services electronically over the internet
vii. **Call Centre Services**: call to call centre agent by clicking on web page.
viii. **Interactive Gaming**: offers consumers a way to meet online and establish interactive gaming sessions.
ix. **Home Manager**: These services could monitor and control home security system, energy system, home entertainment system

NGN Architecture and Network Elements



- **Access Gateways** allows the connection of subscriber lines to the packet network converts the traffic flows of analogue access (Pots) or 2 Mb/s access devices into packets provides subscriber access to NGN network and services.
- **Trunking Gateways** allows interworking between classical TDM telephony network and Packet-based NGN networks, converts TDM circuits/ trunks (64kbps) flows into data packets, and vice versa.
- **Softswitch/MGC** referred to as the Call Agent or Media Gateway Controller (MGC). provides the "service delivery control" within the network in charge of Call Control and handling of Media Gateways control (Access and/or Trunking)
- **Application Server (AS):** A unit that supports service execution, e.g. to control Call Servers and NGN special resources (e.g. media server, message server).
- **Signaling Gateway (SG):** A unit that provides signaling conversion between the NGN and the other networks (e.g. STP in SS7).
- **H.248 Protocol:** Known also as MEGACO: standard protocol, defined by ITU-T, for signaling and session management needed during a communication between a media gateway, and the media gateway controller managing it. H.248/MEGACO allows to set up, keep, and terminate calls between multiple endpoints as between telephone subscribers using the TDM

MPLS

Multiprotocol Label Switching (MPLS) is a protocol for speeding up and shaping network traffic flows. MPLS allows most packets to be forwarded at Layer 2 (the switching level) rather than having to be passed up to Layer 3 (the routing level).

Each packet gets labeled on entry into the service provider's network by the ingress(inlet) router. All the subsequent routing switches perform packet forwarding based only on those labels—they never look as far as the IP header. Finally, the egress(outlet) router removes the label(s) and forwards the original IP packet toward its final destination.

The label determines which pre-determined path the packet will follow. The paths, which are called label-switched paths (LSPs), allow service providers to decide ahead of time what will be the best way for certain types of traffic to flow within a private or public network.

MPLS got its name because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM) and Frame Relay network protocols; any of these protocols can be used to create an LSP. It was created in the late 1990s to avoid having routers waste time by having to stop and look up routing tables. A common misconception is that MPLS is only used on private networks, but the protocol is used for all service provider networks -- including Internet backbones.

In Summary…

In a traditional IP network:

- Each router performs an IP lookup ("routing"), determines a next-hop based on its routing table, and forwards the packet to that next-hop.
- Rinse and repeat for every router, each making its own independent routing decisions, until the final destination is reached.

MPLS does "label switching" instead:

- The first device does a routing lookup.
- But instead of finding a next-hop, it finds the final destination router.
- And it finds a pre-determined path from "here" to that final router.
- The router applies a "label" (or "shim") based on this information.
- Future routers use the label to route the traffic
- Without needing to perform any additional IP lookups.
- At the final destination router, the label is removed.
- And the packet is delivered via normal IP routing.

How does MPLS work?

MPLS works by tagging the traffic, in these example packets, with an Identifier (a Label) to distinguish the LSPs (Label Switched Path- *a specific path between PE (Provider Edge) routers on the MPLS core that the traffic will traverse*). When a packet is received, the router uses this label (and sometimes also the link over which it was received) to identify the LSP. It then looks up the LSP in its own forwarding table to determine the best link over which to forward the packet, and the label to use on this next hop.

A different label is used for each hop, and it is chosen by the router or switch performing the forwarding operation. This allows the use of very fast and simple forwarding engines, which are often implemented in hardware.

Ingress routers at the edge of the MPLS network classify each packet potentially using a range of attributes, not just the packet's destination address, to determine which LSP to use. Inside the network, the MPLS routers use only the LSP labels to forward the packet to the egress router.

- Label Switched Routers (**LSR**) capable of switching and routing packets based on label appended to packet
- Labels define a flow of packets between end points or multicast destinations
- Each distinct flow (forward equivalence class – FEC) has specific path through LSRs (Label Switched Routers) defined - Connection oriented
- Function of LSR are :
  - (i) **PUSH the label** : Adds a new MPLS label to a packet. When a normal IP packet enters an LSP, the new label is the first label on the packet.
  - (ii) **SWAP the label**: Replaces the label with a new label. When an LSR performs an MPLS lookup, that lookup yields the LSP next hop information as well as the numeric identifier for the next segment in the LSP.
  - (iii) **POP the label**: Removes the MPLS label from a packet. This is typically done at the egress (outlet) router.

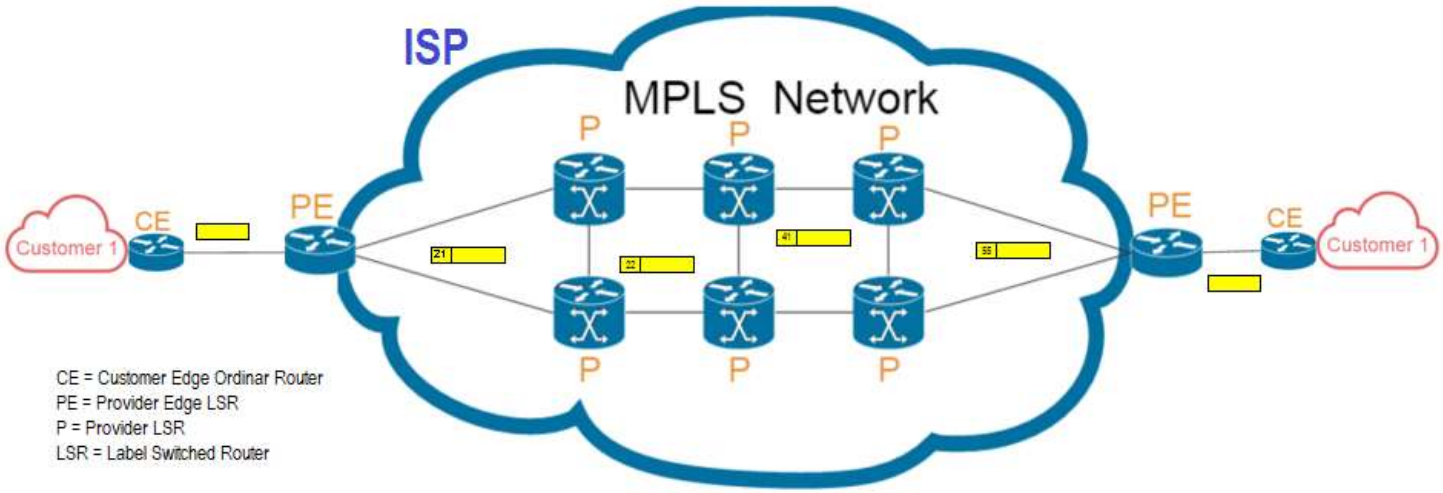


Fig. MPLS

MPLS Benefits

The initial goal of label based switching was to bring the speed of Layer 2 switching to Layer 3. Label based switching methods allow routers to make forwarding decisions based on the contents of a simple label, rather than by performing a complex route lookup based on destination IP address. This initial justification for technologies such as MPLS is no longer perceived as the main benefit, since Layer 3 switches are able to perform route lookups at sufficient speeds to support most interface types.

However, MPLS brings many other benefits to IP-based networks. Forwarding packets based on labels rather than routing them based on headers results in several important advantages:

- `Faster Speed`: Due to the labeling technology, the speed of performing lookups for destinations and routing is much faster than the standard IP table lookups non-MPLS routers have to perform.
- `QoS`: This is a big one. MPLS networks achieve greater Quality of Service for their customers. Quality of Service (QoS) means exactly that – you can expect a higher standard of service such as reliability, speed, and voice quality.
  In addition, MPLS networks are able to assign priorities to the different packets based on what the labels say about that packet. Packets with greater priority, voice over data for example, are given more bandwidth allocation. A packet that which is not deemed as high priority is given less.
- `Faster Restoration`: MPLS networks are also able to restore interrupted connections at a faster speed than typical networks.
- `Security`: MPLS offers greater security and are often required for companies e.g. telecoms which need enhanced privacy and security for their network needs. It's also very popular with organizations that need a scalable WAN that can carry both voice (phone calls) and data.

Assignments

1. You are assigned to design a network infrastructure for a 3-star hotel. Recommend a network solution with hardwares and softwares in current trend that can be used in the hotel. Make necessary assumptions and justify your recommendation with logical arguments where possible.

A network must be able to meet certain criteria, these are mentioned below:

1. Performance
2. Reliability
3. Scalability

Performance

It can be measured in following ways :

- **Transit time :** It is the time taken to travel a message from one device to another.
- **Response time :** It is defined as the time elapsed between enquiry and response.

Other ways to measure performance are :

1. Efficiency of software
2. Number of users
3. Capability of connected hardware

Reliability

It decides the frequency at which network failure take place. More the failures are, less is the network's reliability.

Security

It refers to the protection of data from the unauthorised user or access. While travelling through network, data passes many layers of network, and data can be traced if attempted. Hence security is also a very important characteristic for Networks.

Properties of Good Network

1. **Interpersonal Communication :** We can communicate with each other efficiently and easily example emails, chat rooms, video conferencing etc.
2. **Resources can be shared :** We can use the resources provided by network such as printers etc.
3. **Sharing files, data :** Authorised users are allowed to share the files on the network.

Components of a Network

A computer network comprises the following components:

- ✓ A minimum of at least 2 computers
- ✓ Cables that connect the computers to each other, although wireless communication is becoming more common
- ✓ A network interface device on each computer (this is called a network interface card or NIC)
- ✓ A 'Switch' used to switch the data from one point to another. Hubs are outdated and are little used for new installations.
- ✓ Network operating system software

2. What is computer network? Distinguish between OSI and TCP/IP reference model.
3. What are the features of Client/Server architecture? What are headers and trailers and how do they get added and removed? Explain.

A data packet consists of three elements. The first element is a header, which contains the information needed to get the packet from the source to the destination, and the second element is a data area, which contains the information of the user who caused the creation of the packet. The third element of packet is a trailer, which often contains techniques ensuring that errors do not occur during transmission.

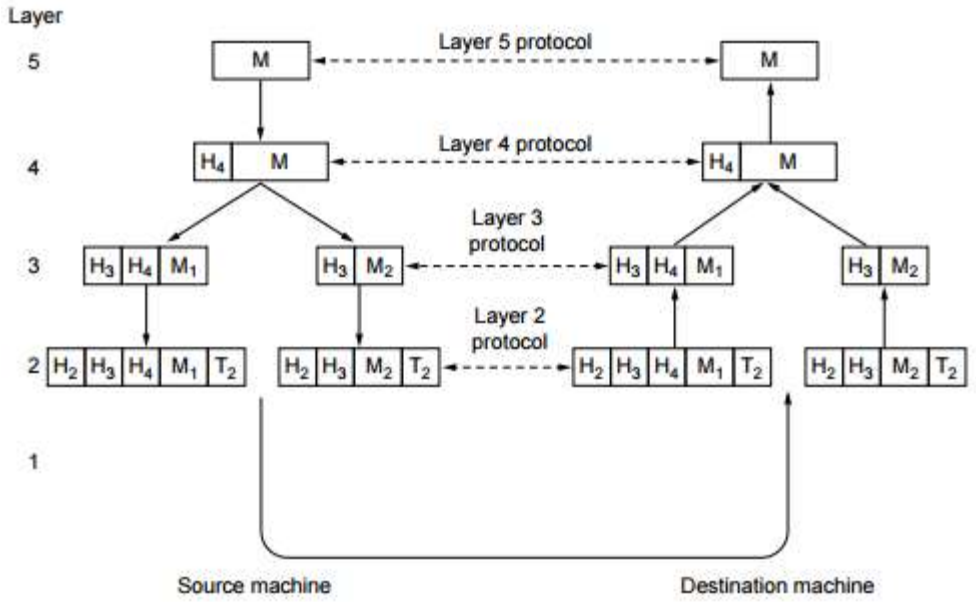
Header &Trailer

A header is attached in the front side or the side which is forward and trailer is at end of each packet, these are control bit not the actual data. Control information means the parity bit or other error detection or correction bits.

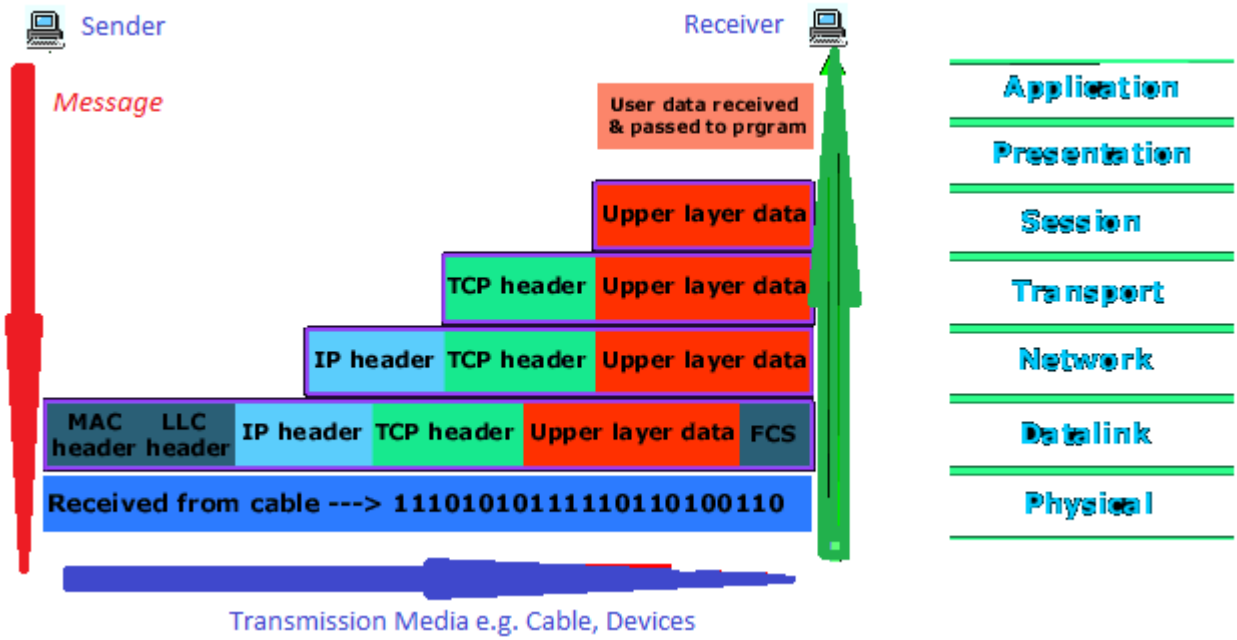
How are they added and removed

The process starts from application layer and moves from layer to layer in descending, sequential order. At each layer a header can be added to the data unit. At layer 2 a trailer is added as well. When the formatted data unit passes through the physical layer (layer 1), it changes into electromagnetic signal and transported along the physical link. Upon reaching the destination, the signal passes into layer 1 and is transformed back into digital

form. The data unit then moves back up through the layers. As each block of data reaches the next higher layer, the header and trailer attached to it at the corresponding sending layer are removed, and actions appropriate to that layer are taken. By the time it reaches the application layer (layer 5), the message is again in a form appropriate to the application and is made available to the recipient.



DATA ENCAPSULATION & DECAPSULATION IN THE OSI MODEL



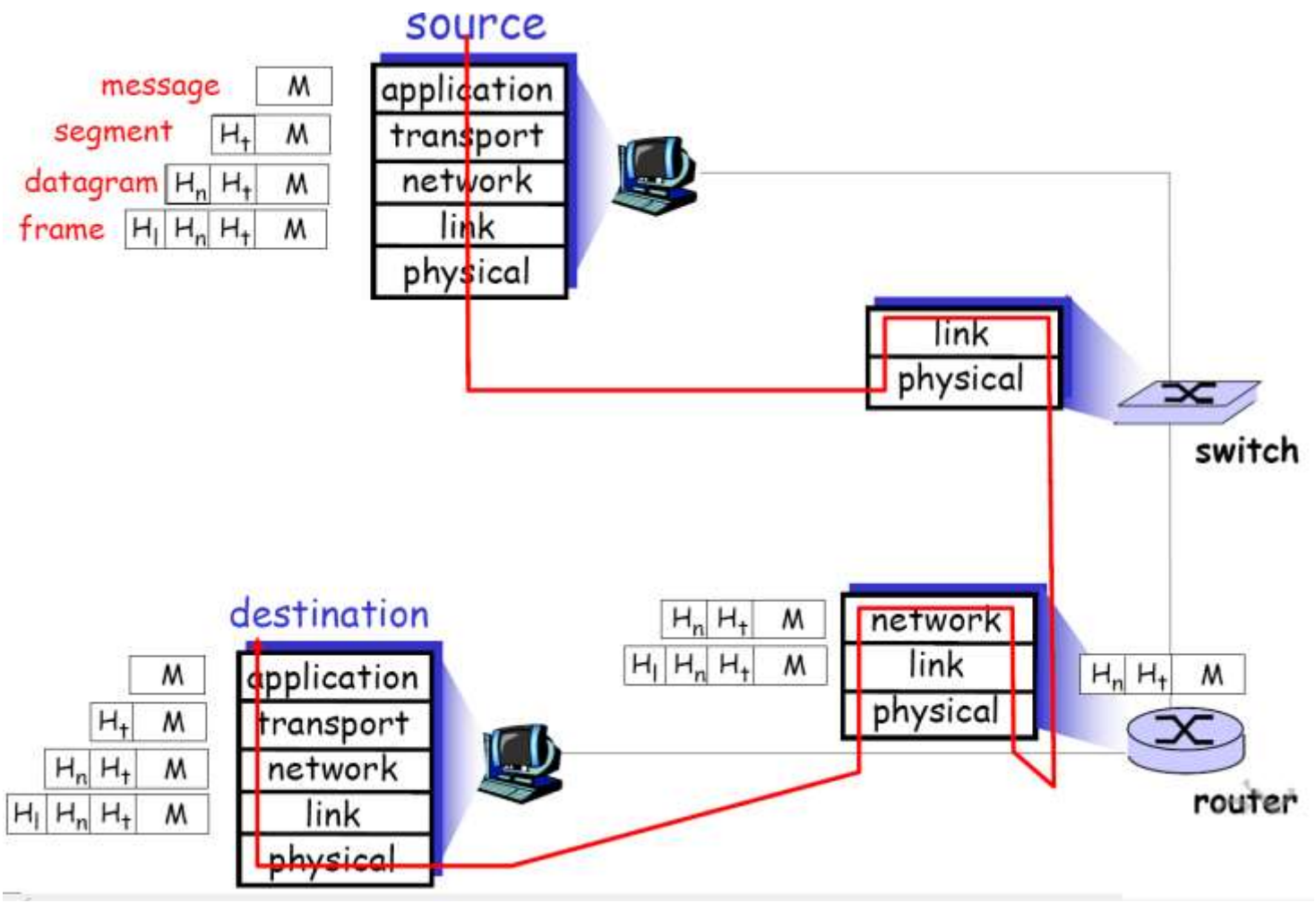


FIG. ENCAPSULATION

We are going to analyse an example in order to try and understand how data encapsulation and decapsulation works. This should make it easier for most people.

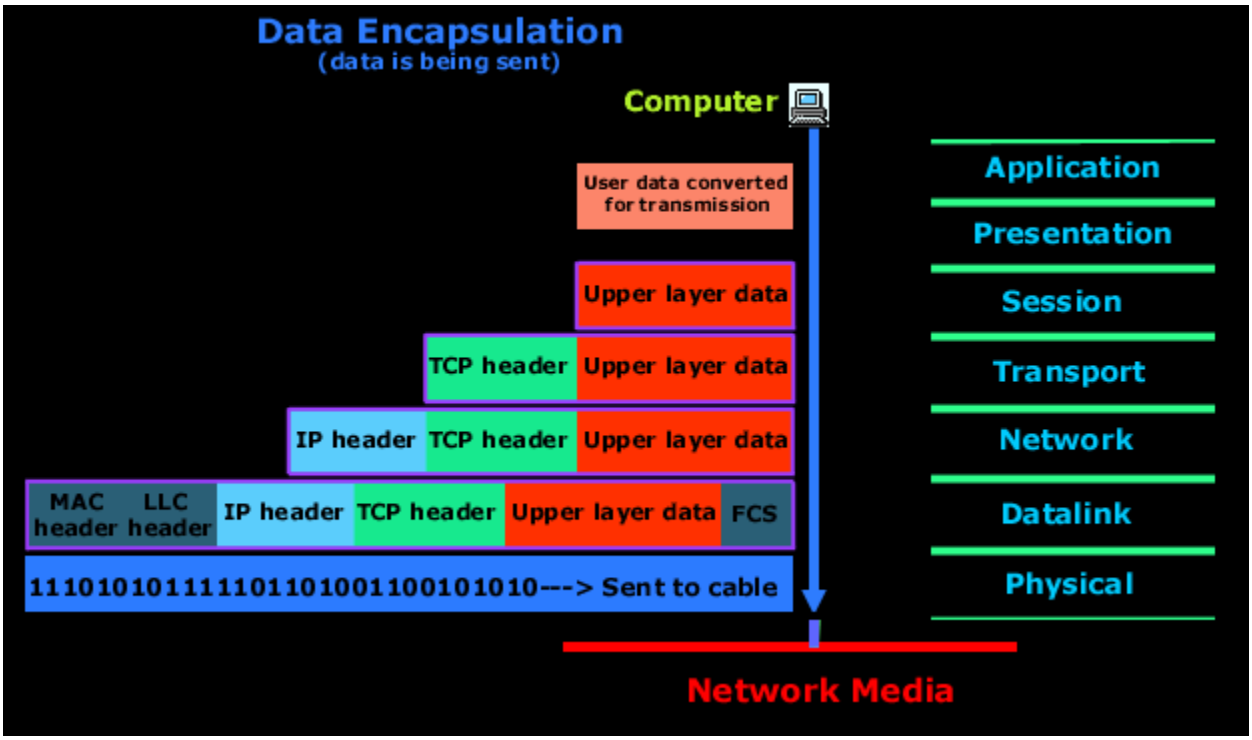
Try to see it this way :

When a car is built in a factory, one person doesn't do all the jobs, rather it's put into a production line and as the car moves through, each person will add different parts to it so when it comes to the end of the production line, it's complete and ready to be sent out to the dealer.

The same story applies for any data which needs to be sent from one computer to another. The OSI model which was created by the IEEE committee is to ensure that everyone follows these guidelines (just like the production line above) and therefore each computer will be able to communicate with every other computer, regardless of whether one computer is a Macintosh and the other is a PC.

One important piece of information to keep in mind is that data flows 2 ways in the OSI model, **DOWN** (**data encapsulation**) and **UP** (**data decapsulation**).

The picture below is an example of a simple data transfer between 2 computers and shows how the data is encapsulated and decapsulated:



EXPLANATION:

The computer in the above picture needs to send some data to another computer. The Application layer is where the user interface exists, here the user interacts with the application he or she is using, then this data is passed to the Presentation layer and then to the Session layer. These three layer add some extra information to the original data that came from the user and then passes it to the Transport layer. Here the data is broken into smaller pieces (one piece at a time transmitted) and the TCP header is a added. At this point, the data at the Transport layer is called a *segment*.

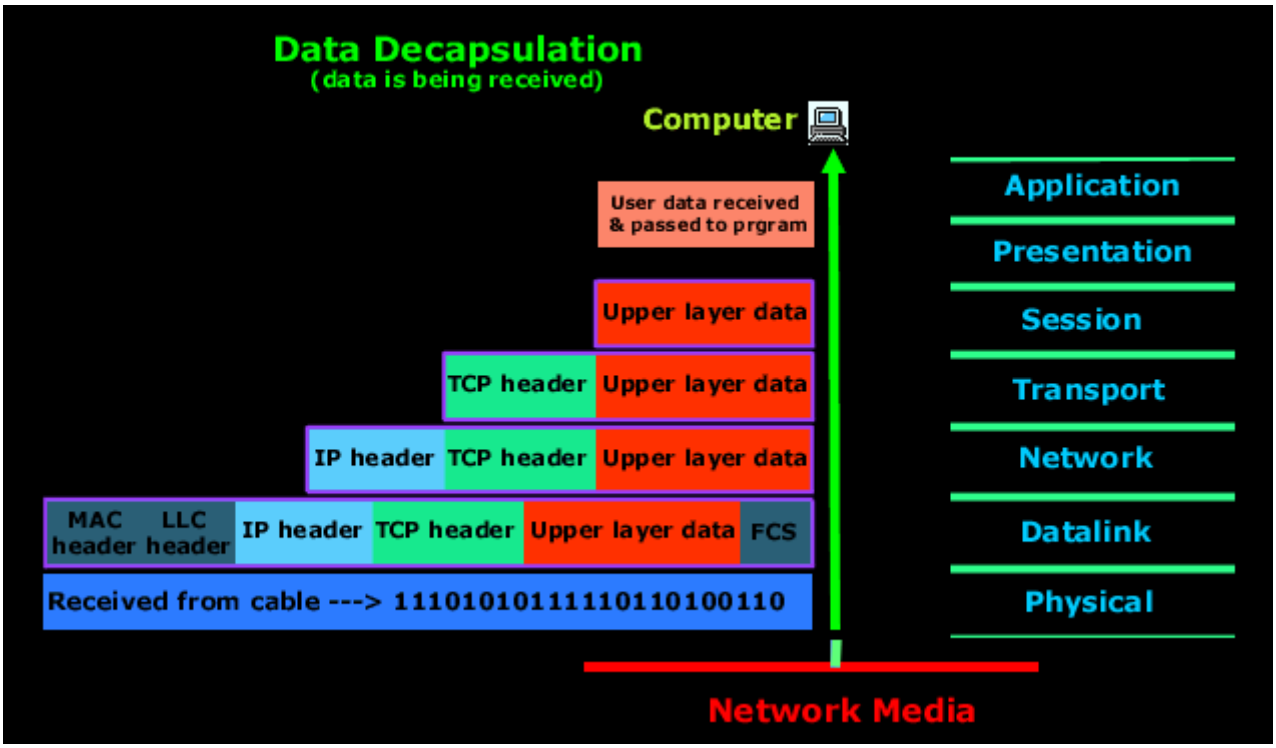
Each segment is sequenced so the data stream can be put back together on the receiving side exactly as transmitted. Each segment is then handed to the Network layer for network addressing (logical addressing) and routing through the internet network. At the Network layer, we call the data (which includes at this point the transport header and the upper layer information) a *packet*.

The Network layer add its IP header and then sends it off to the Datalink layer. Here we call the data (which includes the Network layer header, Transport layer header and upper layer information) a *frame*. The Datalink layer is responsible for taking packets from the Network layer and placing them on the network medium (cable). The Datalink layer encapsulates each packet in a frame which contains the hardware address (MAC) of the source and destination computer (host) and the LLC information which identifies to which protocol in the prevoius layer (Network layer) the packet should be passed when it arrives to its destination. Also, at the end, you will notice the FCS field which is the Frame Check Sequence. This is used for error checking and is also added at the end by the Datalink layer.

If the destination computer is on a remote network, then the frame is sent to the router or gateway to be routed to the desination. To put this frame on the network, it must be put into a digital signal. Since a frame is really a logical group of 1's and 0's, the Physical layer is responsible for encapsulating these digits into a digital signal which is read by devices on the same local network.

There are also a few 1's and 0's put at the begining of the frame, only so the receiving end can synchronize with the digital signal it will be receiving.

Below is a picture of what happens when the data is received at the destination computer.



EXPLANATION

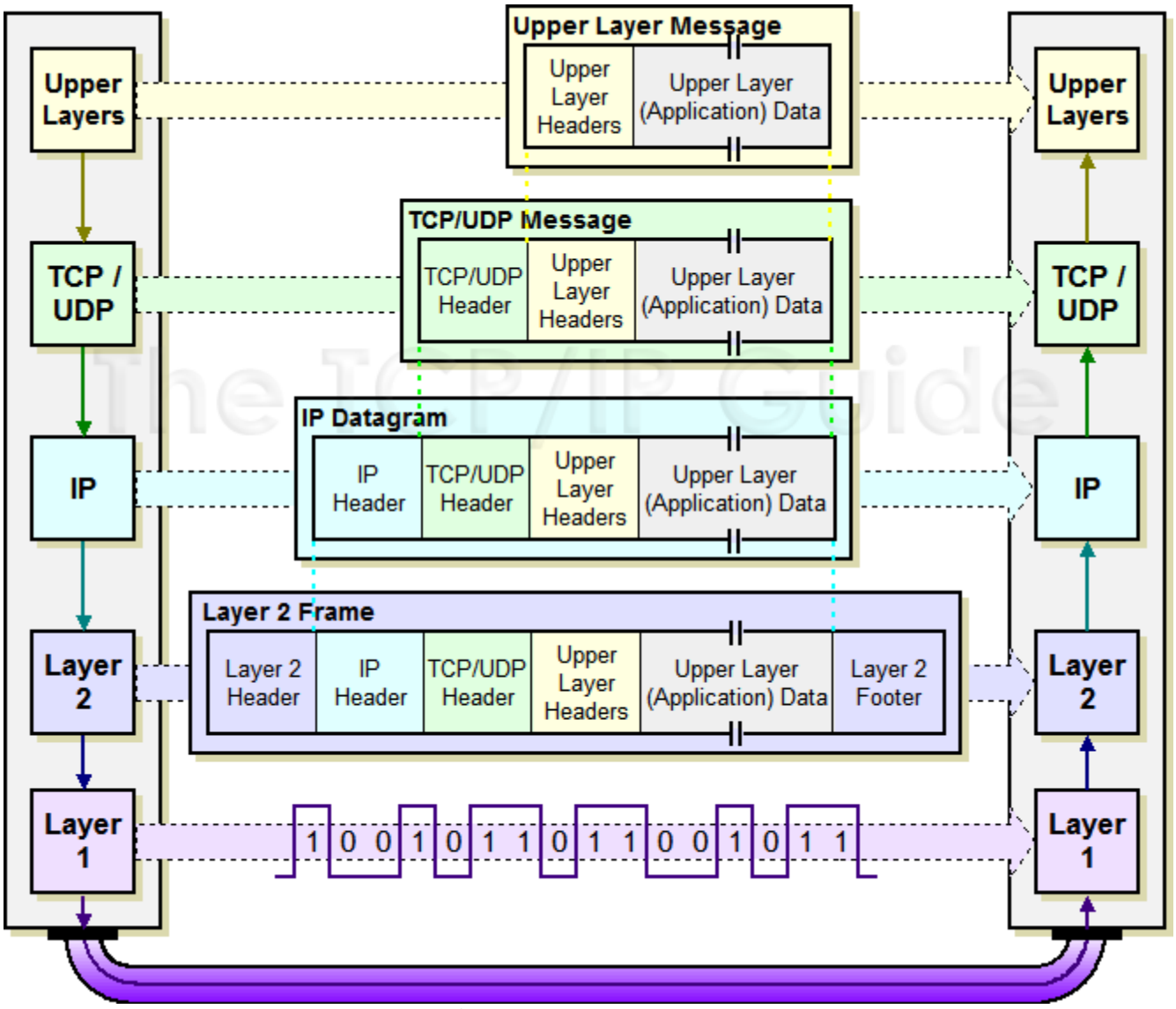
The receiving computer will firstly synchronize with the digital signal by reading the few extra 1's and 0's as mentioned above. Once the synchonization is complete and it receives the whole frame and passes it to the layer above it which is the Datalink layer.

The Datalink layer will do a Cyclic Redundancy Check (CRC) on the frame. This is a computation which the comupter does and if the result it gets matches the value in the FCS field, then it assumes that the frame has been received without any errors. Once that's out of the way, the Datalink layer will strip off any information or header which was put on by the remote system's Datalink layer and pass the rest (now we are moving from the Datalink layer to the Network layer, so we call the data a *packet*) to the above layer which is the Network layer.

At the Network layer the IP address is checked and if it matches (with the machine's own IP address) then the Network layer header, or IP header if you like, is stripped off from the packet and the rest is passed to the above layer which is the Transport layer. Here the rest of the data is now called a *segment*.

The segment is processed at the Transport layer, which rebuilds the data stream (at this level on the sender's computer it was actually split into pieces so they can be transferred) and acknowledges to the transmitting computer that it received each piece. It is obvious that since we are sending an ACK back to the sender from this layer that we are using TCP and not UDP. Please refer to the Protocols section for more clarification. After all that, it then happily hands the data stream to the upper-layer application.

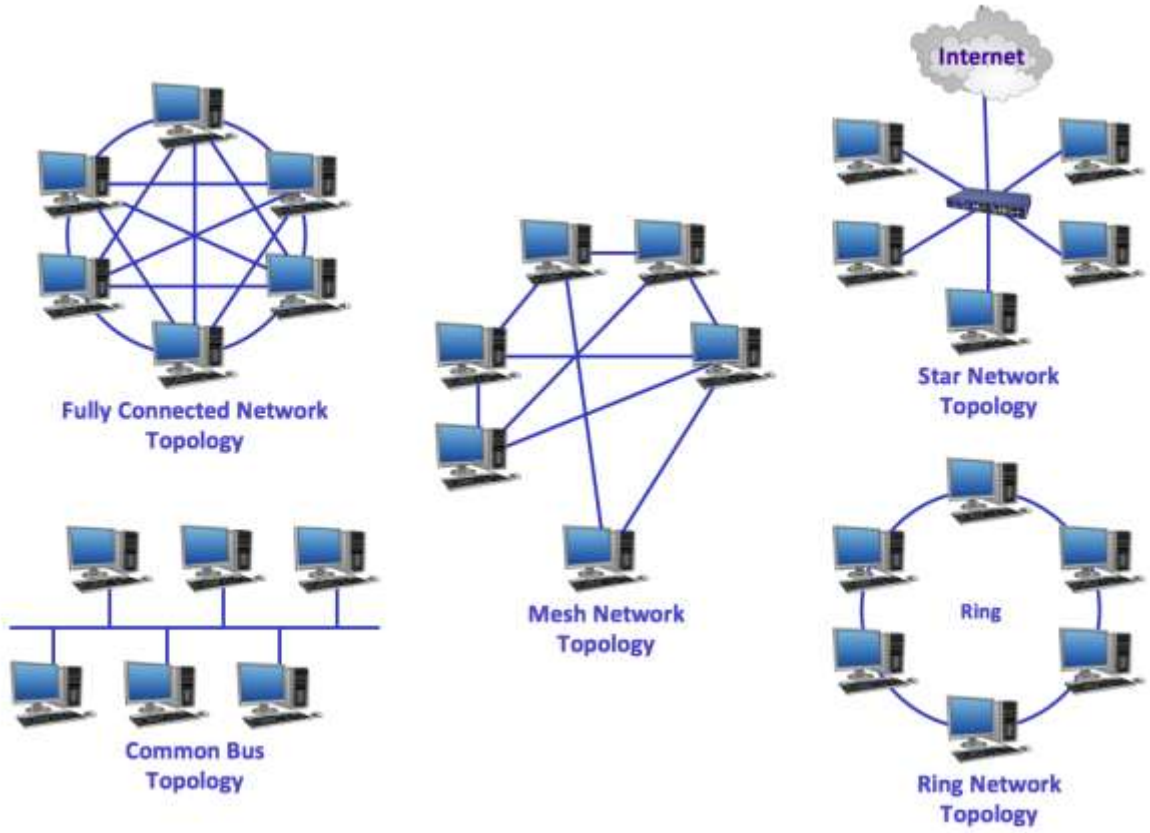
You will find that when analysing the way data travels from one computer to another most people never analyse in detail any layers above the Transport layer. This is because the whole process of getting data from one computer to another involves usually layers 1 to 4 (Physical to Transport) or layer 5 (Session) at the most, depending on the type of data.



how data encapsulation is accomplished in TCP/IP. As you can see, an upper layer message is packaged into a TCP or UDP message. This then becomes the payload of an IP datagram, which is shown here simply with one header (things can get a bit more complex than this.) The IP datagram is then passed down to layer 2 where it is in turn encapsulated into some sort of LAN, WAN or WLAN frame, then converted to bits and transmitted at the physical layer.

4. What do you mean by protocol and interface? Write the protocols used in each layer of TCP/IP model.
5. How do you define network topology? Discuss the types of network topologies based on its size and geographical distribution.

Network topology is the arrangement of the various elements (links, nodes, etc.) of a computer network. An example is a local area network (LAN). Any given node in the LAN has one or more physical links to other devices in the network; graphically mapping these links results in a geometric shape that can be used to describe the physical topology of the network. Conversely, mapping the data flow between the components determines the logical topology of the network.



***Features of Bus Topology**

1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

***Features of Ring Topology**

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.

2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

***Features of Star Topology**

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

***Types of Mesh Topology**

1. **Partial Mesh Topology :** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology :** Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.

Advantages of Mesh Topology

1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

***Features of Tree Topology**

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.

Central hub fails, network fails.

***Features of Hybrid Topology**

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

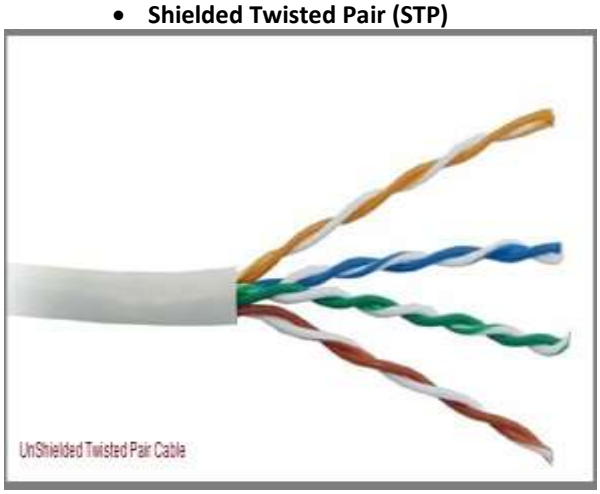
6. Why are the network software defined with distinct layers stacked on top of one another? What are the factors to be considered when designing these layers?
7. Why do we need RAID in the computer network? Define and discuss the differences between RAID 0, RAID 1 and RAID 5.
8. What is X.25? Explain the format of X.25 packet in detail.
9. What are types of twisted pair cable?

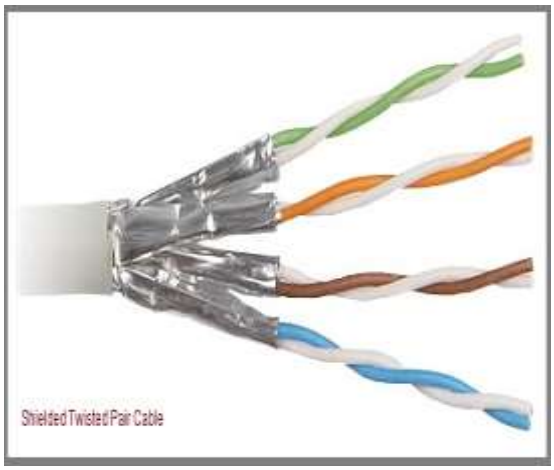
This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points :

- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/Km @ 1kHz.
- Typical delay is 50 µs/km.
- Repeater spacing is 2km.

Twisted Pair is of two types :

- **Unshielded Twisted Pair (UTP)**
- **Shielded Twisted Pair (STP)**





UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use **RJ-11** connector and 4 pair cable use**RJ-45** connector.

10. Why network software should be in hierarchical form? Explain in detail about OSI layer.