Scan or click here for more resources

What is a Network?

- Two or more computers are connected together by a medium and are sharing resources. These resources can be files, printers, hard- drives, or CPU number. It can be done between computers in a home, in a business, across a corporation, and even internationally.
- A network can consist of two computers connected together on a desk, or it can consist of many Local Area Networks (LANs) connected together to form a Wide Area Network (WAN) across a continent.

  Usually, the connections between computers in a network are made using physical wires or cables

  However, some connections are **wireless**, using radio waves or infrared signals.

Importance of Computer Networking

Computer networks have highly benefited various fields of educational sectors, business world and many organizations. They can be seen every where they connect people allover the world. There are some major advantages which compute networks has provided making the human life more relaxed and easy. Some of them are listed below -

Communication

Communication is one of the biggest advantages provided by the computer networks. Different computer networking technology has improved the way of communications people from the same or different organization can communicate in the matter of minutes for collaborating the work activities. In offices and organizations computer networks are serving as the backbone of the daily communication from top to bottom level of organization. Different types of software can be installed which are useful for transmitting messages and emails at fast speed.

Data sharing

Another wonderful advantage of computer networks is the data sharing. All the data such as documents, file, accounts information, reports multi media etc. can be shared with the help computer networks. Hardware sharing and application sharing is also allowed in many organizations such as banks and small firms.

Instant and multiple accesses

Computer networks are multiply processed .many of users can access the same information at the same time. Immediate commands such as printing commands can be made with the help of computer networks.

Video conferencing

Before the arrival of the computer networks there was no concept for the video conferencing. LAN and WAN have made it possible for the organizations and business sectors to call the live video conferencing for important discussions and meetings.

Internet Service

Computer networks provide internet service over the entire network. Every single computer attached to the network can experience the high speed internet. Fast processing and work load distribution

Broad casting

With the help of computer networks news and important messages can be broadcasted just in the matter of seconds who saves a lot of time and effort of the work.

People, can exchange messages immediately over the network any time or we can say 24 hour.

Photographs and large files

Computer network can also be used for sending large data file such as high resolution photographs over the computer network to more then users at a time.

Saves Cost

Computer networks save a lot of cost for any organizations in different ways. Building up links through the computer networks immediately transfers files and messages to the other people which reduced transportation and communication expense. It also raises the standard of the organization because of the advanced technologies that re used in networking.

Remote access and login

Employees of different or same organization connected by the networks can access the networks by simply entering the network remote IP or web remote IP.

Flexible

Computer networks are quite flexible all of its topologies and networking strategies supports addition for extra components and terminals to the network. They are equally fit for large as well as small organizations.

Reliable

Computer networks are reliable when safety of the data is concerned. If one of the attached system collapse same data can be gathered form another system attached to the same network.

Data transmission

Data is transferred at the fast speed even in the scenarios when one or two terminals machine fails to work properly. Data transmission in seldom affected in the computer networks. Almost complete communication can be achieved in critical scenarios too.

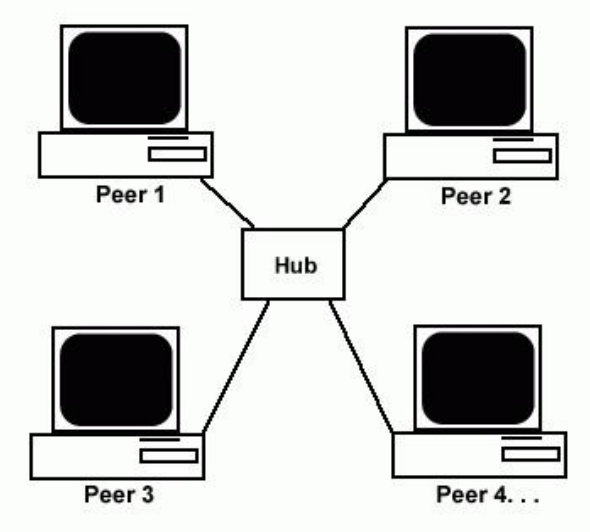
Types of Computer Networks

Networks are all about sharing resources of computers, servers, printers, scanners etc to each other. There are two different types with which network between computers can be formed. Networking formation completely depends on the requirement of the organization scale and usability. We should always study requirements and needs before we decide to choose any type of network. Picking wrong set of options can cost you waste of money, time and resources.

Two types of networks are **Peer to Peer** networking also known to be **p2p**, the other one is **Client and Server networks**.

p2p networking type is most commonly used computer networks. This type of network is very cost effective but supports lesser number of computers in network. Ten to fifteen computers can be connected to each other using p2p networking model without problem, more number of computers often create problems. All computers possesses

same status within the network and no computer control any other computer but it self, this network does not have server to control and monitor. Security level is not towards higher side and each work station it self is responsible for security. Using p2p models files can be shared among computers. Files like, videos, audios, pictures, spreadsheets and all digital media can be sent or received with in the network. Printers, scanners and internet can be shared with in all computers. Below is the picture showing four computers connected to each other with hub and switch. All computers are connected to hub through Network adaptor card using Cable and hub or switch is connected to internet to pass it on to connected computers.. You can see there is no server involved in this diagram but all individual computers are connecting to hub forming P2P network.



Limitation of P2P networking model:

Before deciding to implement P2P model one must know the limitations of this type. Peer to Peer looks very simple, quite cost effective and attractive, yet it can keep progress very limited.

- Peer-To-Peer networks are designed for limited number computers, it will start creating issues when exceed 15 number of computers.

- High security levels can not be achieved using p2p networks, so if organization have concerns with security p2p will not be that great.

- Regular training is required for computer users of p2p network. p2p network is control by computers and computers are controlled by human, small mistake by one of the user can hold the work for other users on same p2p network.

Client Server Network Model :

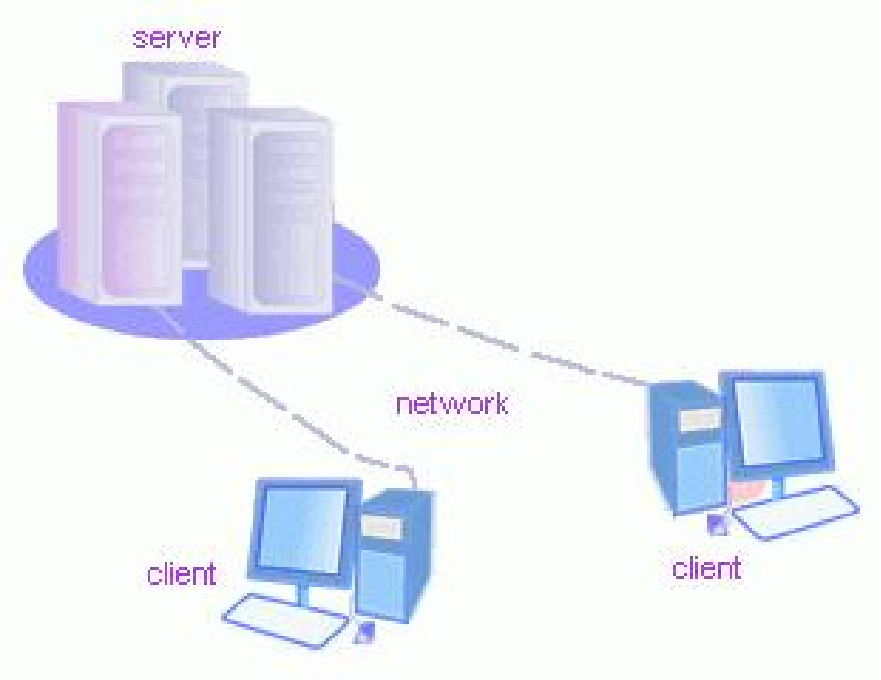
Choosing right kind of networking model is very important for organization. If you are using lesser number of computer and do not see any need to increase the numbers of computers to more than 15 then you are fine with peer to peer networking model, but if you are bigger organization or seeing growth in network, client and server model is designed for it.

The difference in p2p and client server model is that p2p does not have any device or computer that controls computers on network whereas; client / server model has one dedicated computer which is called server. It is called dedicated server. All computers are connected to hub and hub is connected to dedicated server. Server is responsible to perform according to the request sent to it by clients.

For example server can act as print server, if client request a print of document server will send print command to printer and it will be printed. Same way all the files are stored on the server and not on client computer, same client can retrieve data by using any other computer on the same network. This concept is known as centralization, this enables server to keep profile of users, data, and software etc completely in tacked and organized.

Normal computer can also be configured as server and it should be alright and perform server tasks efficiently, but if network growth is on seen and many computers are required to attach to network that's where we might need proper server to take over the network.

You can see in diagram below. All the workstations (Clients) are attached on server, some times there is hub involved but in this case it is just clients and server.



Features of Server:

Servers are powerful machines when they are compared to normal desktop computers. They are meant to provide strength to computing power within the entire network. Controlling developed network can only be done by dedicated servers as they have higher specifications to support network. Servers can have better processing speed with multiple processors capability available. Server machine have higher RAM to load and execute software with ease. They have more advance network cards installed for faster data transfer. Hard drives are way bigger to store the data for entire clients. Hardware can be plugged in and plugged out while server is on, this helps network stable, and hardware like hard disk can be removed and attached accordingly.

Server Os:

Operating systems are also specially designed for servers. Server Os have much more features file serving, print serving, backing up data, enhanced security features etc. There are few major Server Os which are used commonly in servers, Windows server NT. 2000 , 2003,Linux and Novell NetWare. Windows server 2003 is more powerful and enhanced for much higher security levels, Linux servers provide the maximum security to networks.

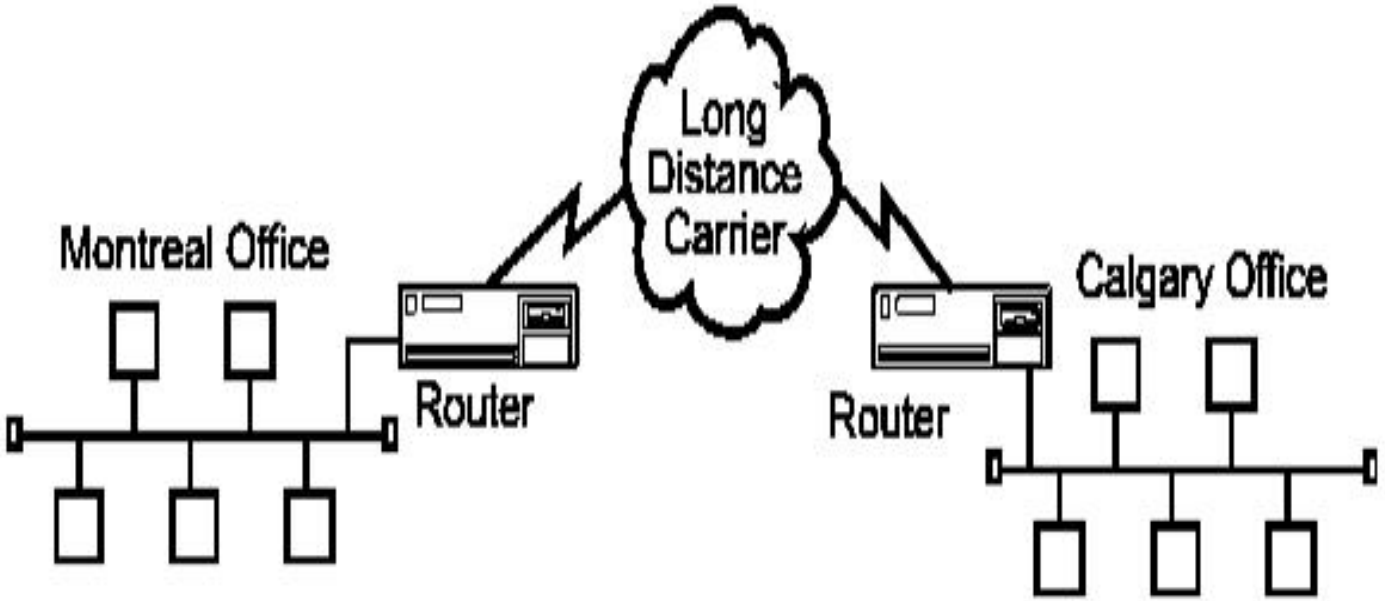
Comptuer Network types

Comptuer networks can be formed, most commonly used is Local Area Networks (**LAN**), others are Wide area network (**WAN**), Metropolitan Area Network (**MAN**).

Local Area Network (LAN) is technical name for computer networks which is normally developed among a single house,office etc. LAN is been implemented and been replaced by WLAN already, WLAN is wireless local area network which performs same function as LAN does but wirelessly. LAN however is still used and understanding it is very important before moving to better and enhance solutions.

Wide Area Network, (WAN) Wide area network is communication among computers which are located far from each other. Internet is one classic example of WAN, It is the collection of large number of computers connecting together to share information with each other and accessible from every where.

WANs connect LANs together between cities



WANs use Long Distance Carriers

Metropolitan Area Network (MAN) Man is not used as commonly as WAN and LAN networks are, it posses its importance when it comes to connect two offices or organization remotely located together to build networks among computing systems. It covers large area but not as much as WAN is capable.

A Metropolitan Area Network is a system of LANs connected throughout a city or metropolitan area. MANs have the requirement of using telecommunication media such as voice channels or data channels. Branch offices are connected to head offices through MANs. Examples of organizations that use MANs are universities and colleges, grocery chains, and banks.

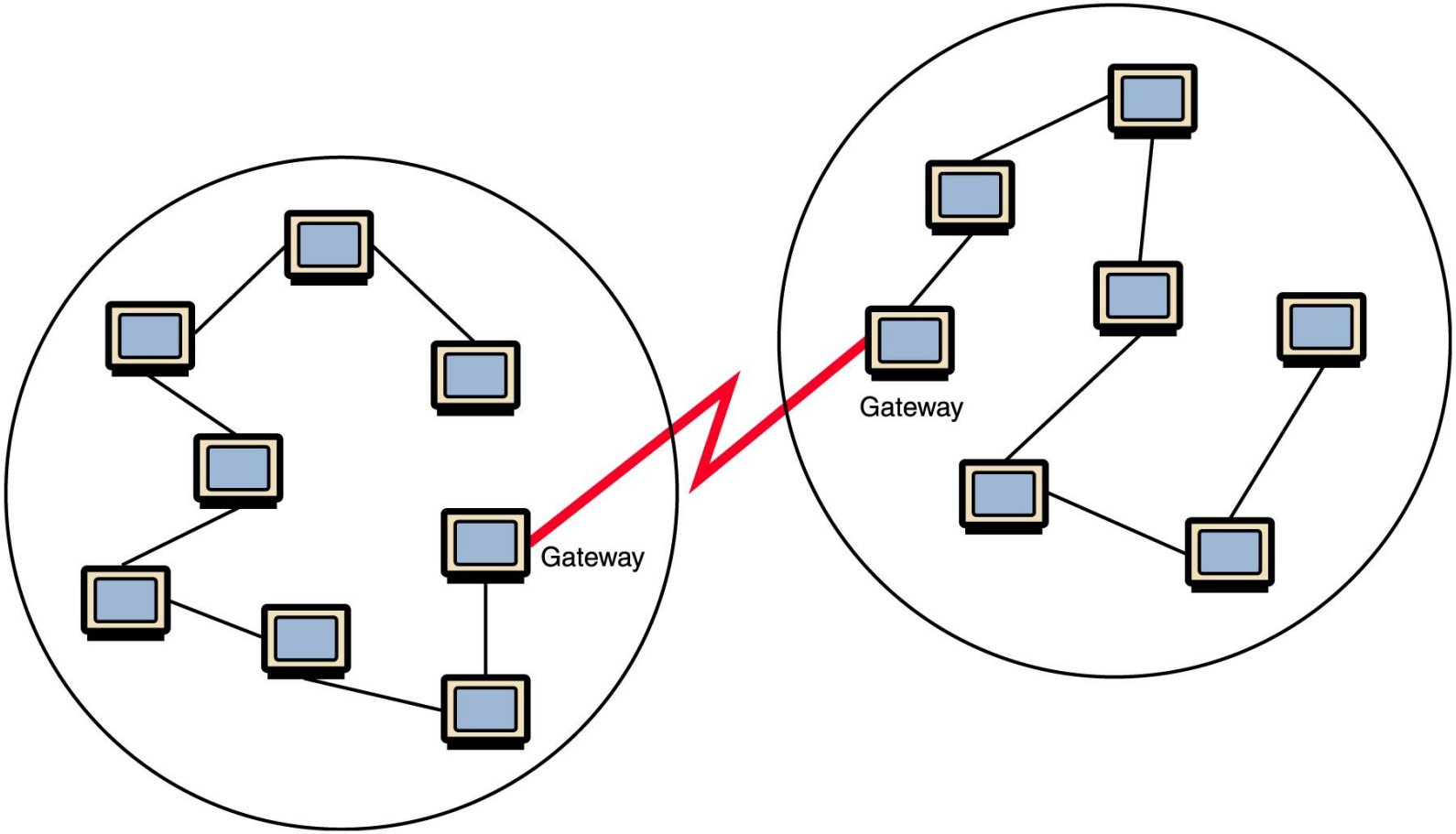
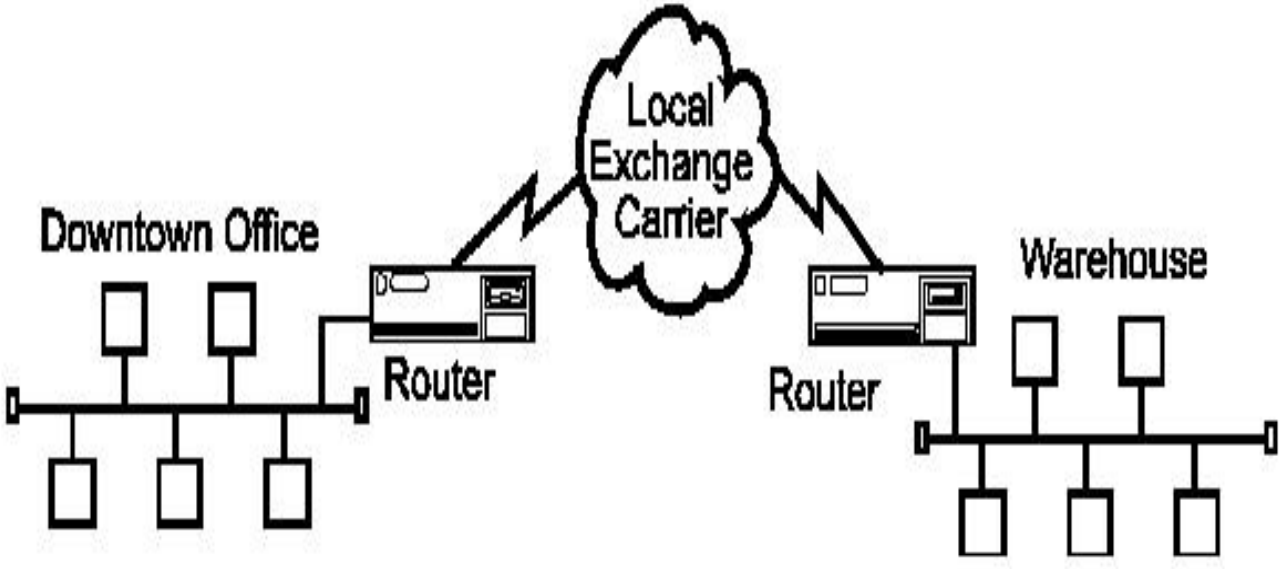


Figure 15.1 **Local-area networks connected across a distance to create a wide-area network**



MANs use Local Exchange Carriers

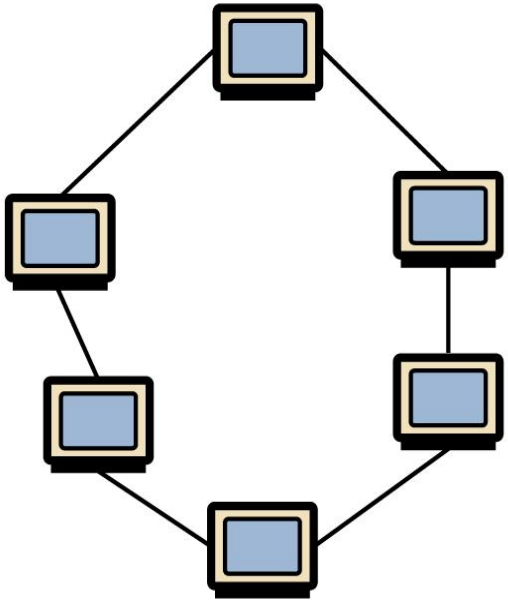
The main criterion for a MAN is that the connection between LANs is through a local exchange carrier (the local phone company). The protocols that are used for MANs are quite different from those used for LANs (except for ATM, which can be used for both under certain conditions).

The main difference between a MAN and a WAN is that the WAN uses Long Distance Carriers. Otherwise the same protocols and equipment are used as a MAN.

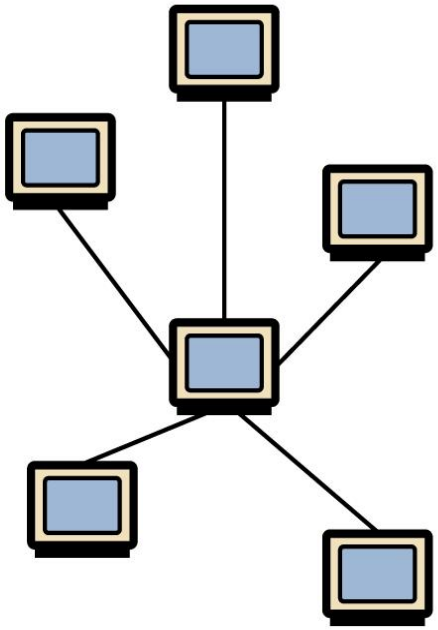
Network Topology

The geometrical representation of relationship of all the link and linking devices to each other called topology.

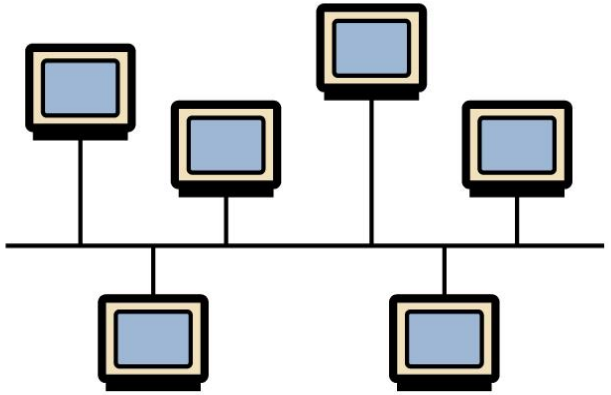
-The geometrical representation of relationship of all the link and linking devices to each other called topology.



Ring topology



Star topology



Bus topology

- A bus technology called **Ethernet** has become the industry standard for local-area networks

Bus Topology

- All nodes are connected to a single communication line that carries messages in both directions.

- Robustness (Strong)

  Good

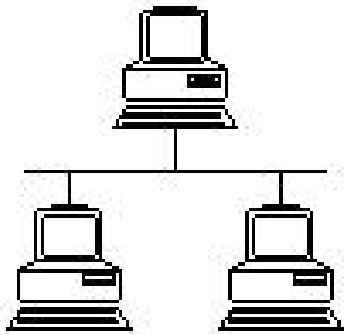
- Efficiency

  Good

- Simplicity

  Excellent

- Easy to connect computer



Ring Topology

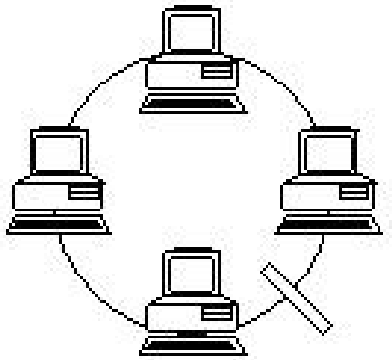
–A configuration that connects all nodes in a closed loop on which messages travel in one direction

- Robustness

  Poor
- Efficiency

  Good
- Simplicity

  Very Good
- Easy to use



Star Topology

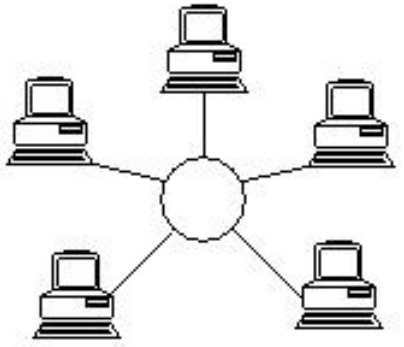
–A configuration that centers around one node to which all others are connected and through which all messages are sent

- Robustness ,means one link fail all other link remain active

  Very Good
- Efficiency

  Very Good
- Easy to install

  Poor
- Less Expensive



- **Tree topology:**

  Combines the properties of star and bus.

Advantages of Networks

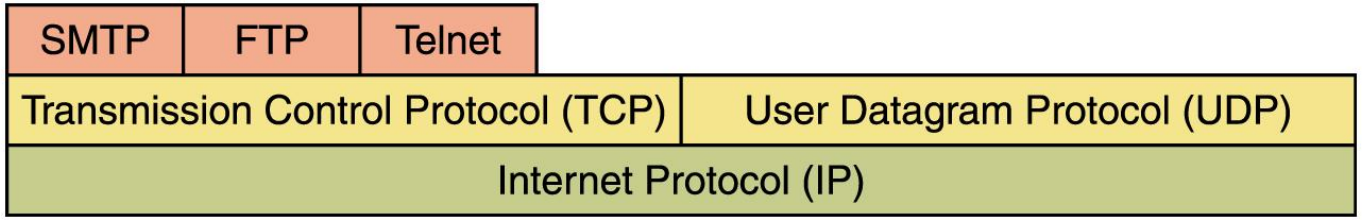
- Performance
- Reliability
- Security

Network Protocol

- Network Protocol is a set of rules that governs the communications between computers on a network. It Represent an agreement between the communicating devices. These rules provide a method for orderly and efficient exchange of data between sender and receiver.

What is a Network Protocol

- Rules of Network Protocol include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer.
- Without protocol two devices may be connected but not communicating just as a person speaking french can not be understand by person who speaks japenese.



Layering of key network protocols

TCP/IP

- TCP stands for **Transmission Control Protocol**

  TCP software breaks messages into packets, hands them off to the IP software for delivery, and then orders and reassembles the packets at their destination. TCP is a connection oriented protocol and offers end-to-end packet delivery. It acts as back bone for connection. It has the following key features: Transmission Control Protocol (TCP) corresponds to the Transport Layer of OSI Model. TCP is a reliable and connection oriented protocol.

TCP offers:

- Stream Data Transfer.
- Reliability.
- Efficient Flow Control
- Full-duplex operation.
- Multiplexing.

- UDP stands for **User Datagram Protocol**
  - It is an alternative to TCP
  - The main difference is that TCP is highly reliable, at the cost of decreased performance, while UDP is less reliable, but generally faster.

- **IP stands for Internet Protocol**

Internet Protocol (**IP**) – A set of rules that dictate how data should be delivered over the public network (**Internet**). Often works in conjunction with the transmission control **protocol** (TCP), which divides traffic into packets for efficient transport through the **Internet**; together they are referred to as TCP/**IP**.

Common **Internet protocols** include TCP/**IP** (Transmission Control **Protocol**/**Internet Protocol**), UDP/**IP** (User Datagram **Protocol**/**Internet Protocol**), HTTP (HyperText Transfer **Protocol**) and FTP (File Transfer **Protocol**).

High-Level Protocols

- Other protocols build on the foundation established by the TCP/IP protocol suite
  - Simple Mail Transfer Protocol (SMTP)
  - File Transfer Protocol (FTP)
  - Telnet
  - Hyper Text Transfer Protocol (http)

Simple Mail Transfer Protocol (SMTP)

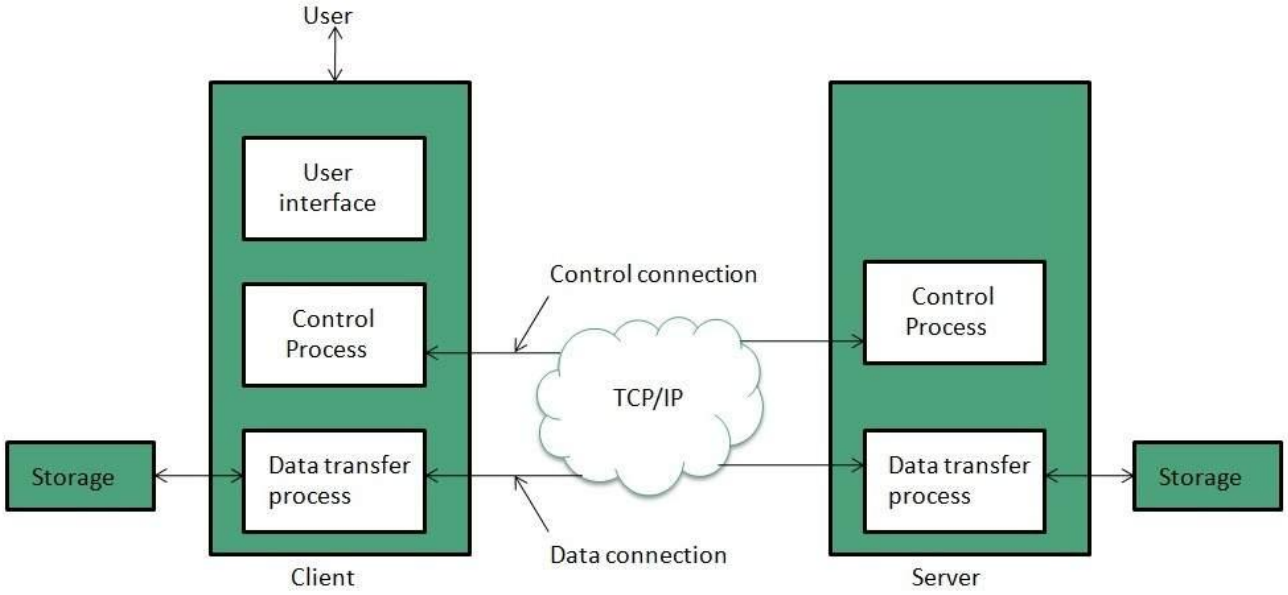
SMTP stands for Simple Mail Transfer Protocol. **SMTP** is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called Simple Mail Transfer Protocol. It is a program used for sending messages to other computer users based on e-mail addresses.

SMTP is part of the application layer of the TCP/IP protocol. Using a process called "store and forward," **SMTP** moves your email on and across networks.

File Transfer Protocol (FTP)

FTP is used to copy files from one host to another. FTP offers the mechanism for the same in following manner:

- FTP creates two processes such as Control Process and Data Transfer Process at both ends i.e. at client as well as at server.
- FTP establishes two different connections: one is for data transfer and other is for control information.
- **Control connection** is made between **control processes.**



Trivial File Transfer Protocol (TFTP)

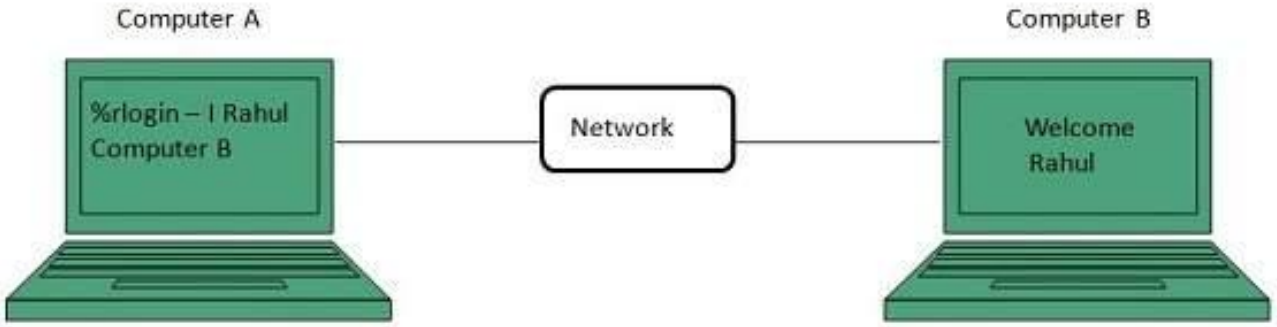
Trivial File Transfer Protocol is also used to transfer the files but it transfers the files without authentication. Unlike FTP, TFTP does not separate control and data information. Since there is no authentication exists, TFTP lacks in security features therefore it is not recommended to use TFTP.

Difference between FTP and TFTP

S.N.	Parameter	FTP	TFTP
1	Operation	Transferring Files	Transferring Files
2	Authentication	Yes	No
3	Protocol	TCP	UDP
4	Control and Data	Separated	Separated
5	Data Transfer	Reliable	Unreliable

Telnet

Telnet is a protocol used to login to remote computer on the internet. There are a number of Telnet clients having user friendly user interface. The following diagram shows a person is logged in to computer A, and from there, he remote logged into computer B.



Hyper Text Transfer Protocol (HTTP)

HTTP is a communication protocol. It defines mechanism for communication between browser and the web server. It is also called request and response protocol because the communication between browser and server takes place in request and response pairs.

HTTP Request

HTTP request comprises of lines which contains:
Request line
Header Fields
Message body

Key Points

- The first line i.e. the **Request line** specifies the request method i.e. **Get** or **Post.**
- The second line specifies the header which indicates the domain name of the server from where index.htm is retrieved.

Roles of a Communication Protocol

A communication protocol normally performs following functions for efficient and error-free transmission of data. It has a separate set of rules for performing each of these functions.

1. **Data Sequencing –** It refers to breaking a long message into smaller packets of fixed size. Data sequencing rules define method of numbering packets to detect loss or duplication of packets.
2. **Data routing –** Data routing rules decide the path between source and destination nodes of a message.
3. **Data formatting –** Data formatting rules define which group of bits or characters within a packet constitutes data, control, addressing or other information.
4. **Flow Control –** They ensure resource sharing and protection against traffic congestion.
5. **Error Control –** Error control rules detect errors in messages to ensure transmission of correct messages.
6. **Precedence and order of transmission –** These rules ensure that all nodes get a chance to use communication lines.

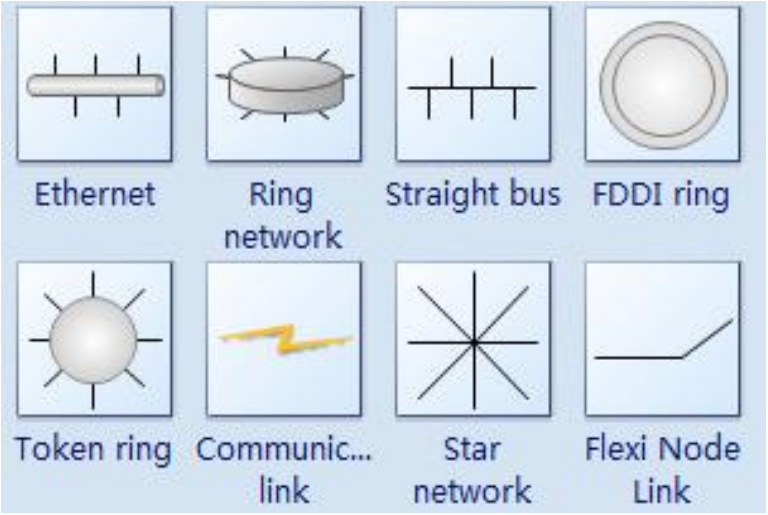
7. **Connection establishment and termination –** These rules define how connections are established, maintained and terminated when two nodes of a network want to communicate with each other.
8. **Data Security –** These rules define mechanisms for providing security and privacy of messages sent/received over the network.

Types of Network Protocols

The most common network protocols are:

- Ethernet
- Local Talk
- Token Ring
- FDDI
- ATM

The followings are some commonly used network symbols to draw different kinds of network protocols.



Ethernet (CSMA/CD):-The Ethernet protocol is by far the most widely used one. Ethernet uses an access method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection). CSMA/CD protocol is one of the popular protocols used for bus topology. The protocol is presented in the following steps –

1. This is a system where each computer listens to the medium(bus) before sending anything through the network.

2. If the network is clear, the computer will transmit.
3. If some other nodes have already transmitted on the cable, the computer will wait and try again when the line is clear.
4. Sometimes, two computers attempt to transmit at the same instant. A collision occurs when this happens. Each computer then backs off and waits a random amount of time before attempting to retransmit.

With this access method, it is normal to have collisions. However, the delay caused by collisions and retransmitting is very small and does not normally effect the speed of transmission on the network.

Fast Ethernet

To allow for an increased speed of transmission, the Ethernet protocol has developed a new standard that supports 100 Mbps, this is commonly called Fast Ethernet. Fast Ethernet requires the application of different, more expensive network hubs and network interface cards. Fast Ethernet is becoming common in schools that have been recently wired. It can be used with both fiber optic cabling .

Gigabit Ethernet

The most latest development in the Ethernet standard is a protocol that has a transmission speed of 1 Gbps. Gigabit Ethernet is primarily used for backbones on a network at this time. In the future, it will probably also be used for workstation and server connections. It can be used with both fiber optic cabling and copper.

FDDI

Fiber Distributed Data Interface (FDDI) is a network protocol that is used primarily to interconnect two or more local area networks, often over large distances. The access method used by FDDI involves token-passing. FDDI uses a dual ring physical topology. Transmission normally occurs on one of the rings; however, if a break occurs, the system keeps information moving by automatically using portions of the second ring to create a new complete ring. A major advantage of FDDI is high speed. It operates over fiber optic cable at 100 Mbps.

ATM

Asynchronous Transfer Mode (ATM) is a network protocol that transmits data at a speed of 155 Mbps and higher. ATM works by transmitting all data in small packets of a fixed size; whereas, other protocols transfer variable length packets. ATM supports a variety of media such as video, CD-quality audio, and imaging. ATM employs a star topology, which can work with fiber optic as well as twisted pair cable.

ATM is most often used to interconnect two or more local area networks. It is also frequently used by Internet Service Providers to utilize high-speed access to the Internet for their clients.

Token Ring

The Token Ring protocol was developed by IBM in the mid-1980s. In Token Ring, the computers are connected so that the signal travels around the network from one computer to another in a logical ring. A single electronic token moves around the ring from one computer to the next. If a computer does not have information to transmit, it simply passes the token on to the next workstation. If a computer wishes to transmit and receives an empty token, it attaches data to the token. The token then proceeds around the ring until it comes to the computer for which the data is meant. At this point, the data is captured by the receiving computer. The Token Ring protocol requires a star-wired ring using twisted pair or fiber optic cable. It can operate at transmission speeds of 4 Mbps or 16 Mbps. Due to the increasing popularity of Ethernet, the use of Token Ring in school environments has decreased.

Data flow in Network

- Simplex mode
- Half Duplex
- Full Duplex

DATA TRANSMISSION MODES

The three modes of data transmission are simplex, half-duplex, and full-duplex.

1. **Simplex –** A simplex communication system can transmit data in one direction only. It is suitable for connecting send-only or receive-only devices. Hence, simplex circuits are less used.
2. **Half-duplex –** A half-duplex communication system can transmit data in both directions, but in only one direction at a time. Hence, it can alternately send and receive data. It requires two wires. It is suitable for voice communication using telephones in which only one person speaks at a time.
3. **Full-duplex –** A full-duplex communication system, which allows data to flow in both directions simultaneously. It requires four wires. It improve efficiency because it eliminates the direction switching delay of a half-duplex system.

DATA TRANSMISSION SPEED

Bandwidth of a communication system refers to its data transfer rate i.e. amount of data that it can transfer per unit of time. Higher the bandwidth of a communication system, the more data it can transfer in a given time. Bandwidth is measured in bits per second (bps) also called baud. Based on data transmission speeds, three basic categories of communication channels or path are :

1. **Narrowband –** Narrowband or sub-voice grade channels have speed in the range of 45 to 300 baud such as telegraph lines use narrowband channels.
2. **Voice-band-** Voice–band channels have speed up to 9600 baud. Their major application is in ordinary telephone voice communication.
3. **Broadband –** Broadband channels have speed of 1 million baud or more. Communication systems for transmission of large volumes of data at high speed use broadband channels.

DATA TRANSMISSION SERVICES

A data transmission path between two computer located far away from each other often involves multiple data transmission media such as copper wire, fiber optic cable and communication satellite. Organisation hire services of data-transmission-services providers known as common carriers such as VSNL (Videsh Sanchar Nigam Limited), BSNL (Bharat Sanchar Nigam Limited) and MTNL (Mahanagar Telephone Nigam Ltd.) are in India whereas At&T, MCI, Western Union and GTE are in USA. Typically, common carriers offer following types of services –

1. **Dial-up line–** Dial-up line services operates like a telephone service. A computer user willing to communicate with a remote first makes a connection request by dialing up the remote computer. The communication system then establishes a circuit between the two computers via telephone company's switching system. Modems attached to the computer then send and receive data over telephone line.

2. **Leased line-** Leased line is a special conditioned telephone line connecting two computers or two line terminating equipment like routers directly and permanently. It can transmit both voice and data. Charges for a leased line are based on channel capacity (bps) and distance.

3. **Integrated Services Digital Network (ISDN)–** The ISDN is a telephonic system providing digital telephone and data services. ISDN telephone users enjoy noise-free, CD-equality, sound. Moreover, ISDN does not require modems because it supports digital transmission of all types of data.

4. **Value Added Network (VAN)–** Some companies specialize in providing value added data transmission service over and above the standard services of common carriers. Value-added services include electronic mail, data encryption/decryption, access to commercial databases and code conversion for communication between incompatible computers.

ASYNCHRONOUS AND SYNCHRONOUS TRANSMISSION

Two modes of data transmission on a communication channel are asynchronous and synchronous-

ASYNCHRONOUS TRANSMISSION

In asynchronous transmission, a communication system transmits data character by character at irregular intervals i.e. a sender sends a character at any convenient time and receiver accepts. To enable a receiver to recognize a character when it arrives, a transmitter frames each character by putting a start bit before it and one or two stop bits it. Hence , for 7-bit ASCII code, for each character a transmitter transmits 10 or 11 bits (7 character bits, 1 parity bit, 1 start bit and 1 or 2 stop bits.)

Its advantages is that it does not require any local storage at sender or receiver end, because transmission takes place character by character. Hence it is cheaper to implement.

SYNCHRONOUS TRANSMISSION

In synchronous transmission, a communication system groups character into blocks and then adds a header and trailer to each block to convert it into a frame. The header contains synchronization information, which receiving device uses to set its clock in synchronism with sender end clock. The number of character in a block may be variable. And may consist of hundreds of characters. A trailer terminates the message character of a block. The trailer contains and end-of-message character. Hence, in synchronous transmission, a communication system frames an entire block of character and then transmits it at a time.

Synchronous transmission is suitable for communication between buffered devices. Synchronous transmission has much higher data transmission rates than asynchronous transmission, because it eliminates need for individual start-stop bits for each character.

TRANSMISSION MEDIA (NETWORK CABLES)

Some popular data transmission media are as follows-

1. **Twisted-Pair Wire–** A twisted-pair wire consists of two bunches of thin copper wires, each bunch enclosed separately in a plastic insulation, then twisted around each other to reduce interference by adjacent wires. It is also called unshielded twisted-pair (UTP) cable. UTP cable are used commonly in local telephone communication and short distance upto 1 km. For distance upto 100 mt, they provide data transmission speed of upto 9600 bps and for longer distance they provide speed of the order of 1200 bps. UTP cables are inexpensive and easy to install and use. However their use is limited because they easily pick up noise signals when line length extends beyond 100 mt.

2. Coaxial Cable- Coaxial cables consist of a central copper wire surrounded by a PVC insulation over which there is a sleeve of copper mesh. The copper mesh sleeve is shielded again by an outer shield of thick PVC material. Signal is transmitted by inner copper wire, and is electrically shielded by the outer copper mesh sleeve. Coaxial cables offer much higher bandwidths than UTP cables, and can transmit digital signals at rates upto 10 mega bps. They are used extensively in long distance telephone lines for both voice and data transmission.

3. Microwave System- Microwave systems are use very high frequency ratio signals to transmit data through space (wireless communication). However, at microwave frequencies, electromagnetic waves cannot bend or pass like tall building or hills. Hence, transmitter and receiver of a microwave system, mounted on very high towers, should be in line-of-sight. To overcome problems of line-of-sight and power amplification of weak signals, microwave systems use repeaters at intervals of about 25 to 30 kms in between transmitting and receiving stations.

4. Optical Fibers– Optical fibers are made of glass, plastic or silica. Plastic fibers are least efficient but are cheaper. Glass or silica fibers are much smaller and more suitable for high capacity channels.

Physically, a fiber-optical cable consists of three concentric layers – inner core, a cladding around it and outer protective coating. Inner core has a diameter of 8 to 200 micrometers and consists of a bunch of optical fibers. The cladding around it is made of plastic or glass.

Optical fibers have following advantages –

- Large Bandwidth
- Low loss
- Immunity to electromagnetic interference
- Small size and lightweight
- Security
- Safety and electrical insulation
- Analog and digital signals transmission

5. **Communication Satellite–** Communication satellites are microwave relay stations in outer space. A space launches a satellite and places it in outer space 36,000 kms above the equator with an orbit speed that matches earth's rotation speed exactly.

Satellite communication systems have following advantages –

- A satellite is essentially a microwave relay station visible from any point in a very large area.
- Data transmission costs are independent of distance between two points as long as these two points are within the satellite's area coverage.
- A satellite having many transponders has enormous data communication capability.
- As they support wireless communication, they do not require laying of cables.

Satellite communication systems have following disadvantages –

- Initial cost of placing a satellite into its orbit is very high.
- Data propagation delay of about 270 msec between sender and receiver.
- Whatever data a satellite receives for transmission, it broadcasts it automatically to all receiving stations within the satellite's area coverage.
- Atmospheric disturbances like thunder and lightening affect transmission of a satellite communication system.

ISO/OSI Model

- The International Standards Organization (ISO) Open Systems Interconnect (OSI) is a standard set of rules describing the transfer of data between each layer in a network operating system. Each layer has a specific function. For example, the physical layer deals with the electrical and cable specifications.

- The OSI Model clearly defines the interfaces between each layer. This allows different network operating systems and protocols to work together with the standard interfaces. The application of the ISO/OSI model has allowed the modern multi-protocol networks that exist today.

The OSI Reference Model

Principles for the seven layers

- Each layer performs well-defined function.
- Function of layer chosen with definition of international standard protocols in mind.
- Minimize information flow across interfaces between boundaries.
- Number of layers optimum.

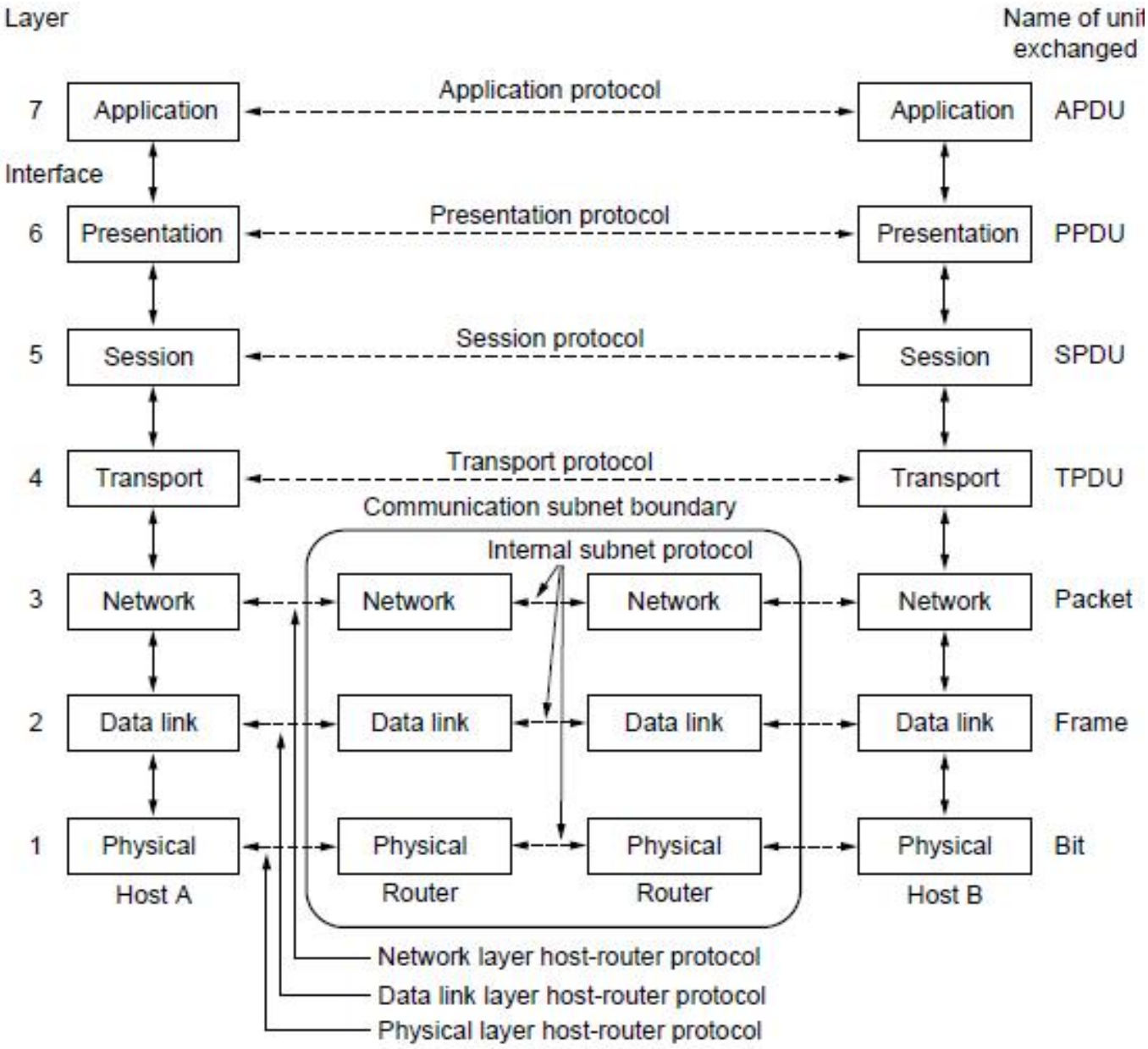
Seven Layers in the OSI Model

- 7. Application Layer (Top Layer)
- 6. Presentation Layer
- 5. Session Layer
- 4. Transport Layer
- 3. Network Layer
- 2. Data Link Layer
- 1. Physical Layer (Bottom Layer)

7 Layers

7.	Application Layer	All
6.	Presentation Layer	People
5.	Session Layer	Seem
4.	Transport Layer	To
3.	Network Layer	Need
2.	Data Link Layer	Data
1.	Physical Layer	Processing

The OSI Reference Model



LAYER 7 – The APPLICATION Layer

- The application layer is responsible for providing services to the user.
- The top layer of the OSI model
- The major role of application layer is to provide the facility to use the other layers. It contains several protocols that are generally needed to perform a job. The contents of the application layer are determined by the user themselves.
- Provides a set of interfaces for sending and receiving applications to gain access to and use network services, such as: networked file transfer, message handling and database query processing

LAYER 6 – The PRESENTATION Layer

- The presentation layer is responsible for translation, compression, and encryption.
- This layer serves as an interface between the application and the communication network. Typical function of this layer is to code the data into mutually agreed formats. The presentation layer performs the compression of data and forms a sequence of symbols according to the standard format.
- For outgoing messages, it converts data into a generic format for network transmission; for incoming messages, it converts data from the generic network format to a format that the receiving application can understand
- This layer is also responsible for certain protocol conversions, data encryption/decryption, or data compression/decompression

LAYER 5 – The SESSION Layer

- Enables two networked resources to hold ongoing communications (called a session) across a network.
- Session layer provides means of establishing, maintaining and terminating a session between two end users. It allow communication parties to authenticate each other before establishing a dialog session between them. It specifies dialog type – one-way, two-way and initiates a dialog session, It also provides priority management service that is useful for giving priority to important and time-bound message over normal, less important messages.
- Applications on either end of the session are able to exchange data for the duration of the session.

LAYER 4 – The TRANSPORT Layer

- The transport layer is responsible for the delivery of a message from one process to another.
- Role of transport layer is to receive the data from session layer and divide it into pieces in order to pass it to network layer.
- A major function of this layer is to hide the details of communication network and provide a network independent device-to-device communication.
- Manages the transmission of data across a network
- Reassembles chunks into their original sequence at the receiving end

LAYER 3 – The NETWORK Layer

- The network layer is responsible for the delivery of individual packets from the source host to the destination host.
- Handles addressing messages for delivery, as well as translating logical network addresses and names into their physical counterparts
- Responsible for deciding how to route transmissions between computers
- This layer also handles the decisions needed to get data from one point to the next point along a network path
- This layer also handles packet switching and network congestion control

LAYER 2 – The DATA LINK Layer

- The function of this layer is to recover from the transmission errors. Data link layer takes care of the speed mismatch between senders and receivers. Any disparity in the speed of sending a data and receiving it is taken care by data link layer.
- Handles special data frames (packets) between the Network layer and the Physical layer
- At the receiving end, this layer packages raw data from the physical layer into data frames for delivery to the Network layer
- At the sending end this layer handles conversion of data into raw formats that can be handled by the Physical Layer

LAYER 1 – The PHYSICAL Layer

- The physical layer is responsible for movements of individual bits from one node to the next.
- Converts bits into electronic signals for outgoing messages.
- Converts electronic signals into bits for incoming messages.
- This layer manages the interface between the computer and the network medium (coax, twisted pair, etc.)
- The bottom layer of the OSI model.