- ***Data*** generally are defined as information that is stored in digital form.
- ***Information*** is defined as the knowledge or intelligence.
- ***Data communications*** is transmission, reception, and processing of digital information.
- ***NOTE: (Data is a plural word , datum is a singular word .)***

Standards Organizations for Data Communications:

An association of organizations, governments, manufacturers and users form the standards organizations and are responsible for developing, coordinating and maintaining the standards .The purpose is that all data communications equipment manufacturers and users comply with these standards. The primary standards organizations for data communication are:

1. International Standard Organization (ISO)

ISO is the international organization for standardization on a wide range of subjects. It is comprised mainly of members from the standards committee of various governments throughout the world. It is even responsible for developing models which provides high level of system compatibility, quality enhancement, improved productivity and reduced costs. The ISO is also responsible for endorsing and coordinating the work of the other standards organizations.

2. International Telecommunications Union-Telecommunication Sector (ITU-T)

ITU-T is one of the four permanent parts of the International Telecommunications Union based in Geneva, Switzerland. It has developed three sets of specifications: the *V series* for modem interfacing and data transmission over telephone lines, the *X series* for data transmission over public digital networks, email and directory services; the *I and Q series* for Integrated Services Digital Network (ISDN) and its extension Broadband ISDN. ITU-T membership consists of government authorities and representatives from many countries and it is the present standards organization for the United Nations.

3. Institute of Electrical and Electronics Engineers (IEEE)

IEEE is an international professional organization founded in United States and is compromised of electronics, computer and communications engineers. It is currently the world's largest professional society with over 200,000 members. It develops communication and information processing

standards with the underlying goal of advancing theory, creativity, and product quality in any field related to electrical engineering.

4. American National Standards Institute (ANSI)

ANSI is the official standards agency for the United States and is the U.S voting representative for the ISO. ANSI is a completely private, non-profit organization comprised of equipment manufacturers and users of data processing equipment and services. ANSI membership is comprised of people form professional societies, industry associations, governmental and regulatory bodies, and consumer goods.

5. Electronics Industry Association (EIA)

EIA is a non-profit U.S. trade association that establishes and recommends industrial standards. EIA activities include standards development, increasing public awareness, and lobbying and it is responsible for developing the RS (recommended standard) series of standards for data and communications.

6. Telecommunications Industry Association (TIA)

TIA is the leading trade association in the communications and information technology industry. It facilitates business development opportunities through market development, trade promotion, trade shows, and standards development. It represents manufacturers of communications and information technology products and also facilitates the convergence of new communications networks.

7. Internet Architecture Board (IAB)

IAB earlier known as Internet Activities Board is a committee created by ARPA (Advanced Research Projects Agency) so as to analyze the activities of ARPANET whose purpose is to accelerate the advancement of technologies useful for U.S military. IAB is a technical advisory group of the Internet Society and its responsibilities are:

I. Oversees the architecture protocols and procedures used by the Internet.

II. Manages the processes used to create Internet Standards and also serves as an appeal board for complaints regarding improper execution of standardization process.

III. Responsible for administration of the various Internet assigned numbers

IV. Acts as a representative for Internet Society interest in liaison relationships with other organizations.

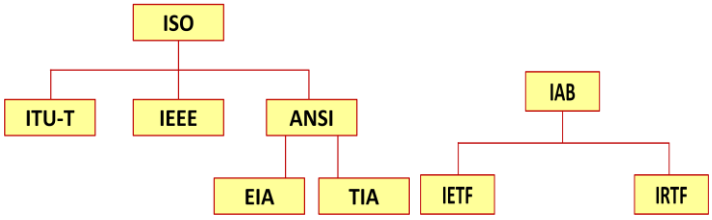
V. Acts as a source of advice and guidance to the board of trustees and officers of Internet Society concerning various aspects of internet and its technologies.

8. Internet Engineering Task Force (IETF)

The IETF is a large international community of network designers, operators, vendors and researchers concerned with the evolution of the Internet architecture and smooth operation of the Internet.

9. Internet Research Task Force (IRTF)

The IRTF promotes research of importance to the evolution of the future Internet by creating focused, long-term and small research groups working on topics related to Internet protocols, applications, architecture and technology.



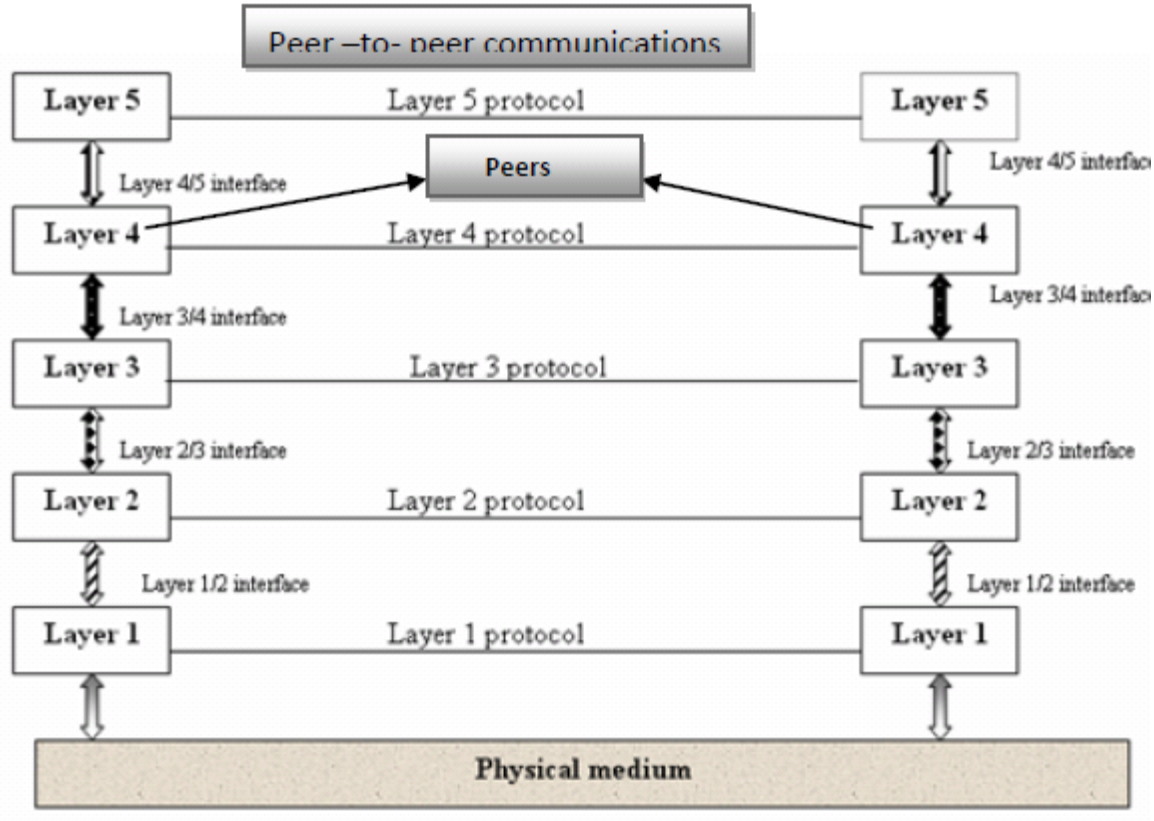
Layered Network Architecture

To reduce the design complexity, most of the data communication networks are organized as a series of **layers** or **levels**, each one build upon one below it ***(Divide and Rule Policy)***. The basic idea of a layered architecture is to divide the design into small pieces. Each layer adds to the services provided by the lower layers.

Advantages of Layered Network Architecture:

- Design Complexity of data communication networks is reduced.
- If you make any changes in a layer, it does not affect other layers.(This is called modularity between layers)

- **Peer to Peer to Communication**: A given layer in one system can **logically** communicate with corresponding layer in another system. Different Computers can communicate logically at different layers or levels.



Disadvantages of Layered Network Architecture:

- Huge amount of overhead

Basic elements of a layered Network Architecture

- Services.
- Protocols.
- Interfaces.

A ***service*** is a set of actions that a layer offers to another (higher) layer.

Protocol is a set of rules that a layer uses to exchange information

Interface: Between the layers service interfaces are defined. The messages from one layer to another are sent through those interfaces.

Protocol Data Unit (PDU):

PDU is a unit of data used for communication between two corresponding layers.

- Data flows downward through the layers in the source system
- Data flows upwards at the destination address.
- In intermediate systems data flows upward first and then downward (In a data communication network, between source and destination there are many systems. Those are called intermediate systems)
- As data passes from one layer into another, headers and trailers are added and removed from the PDU.

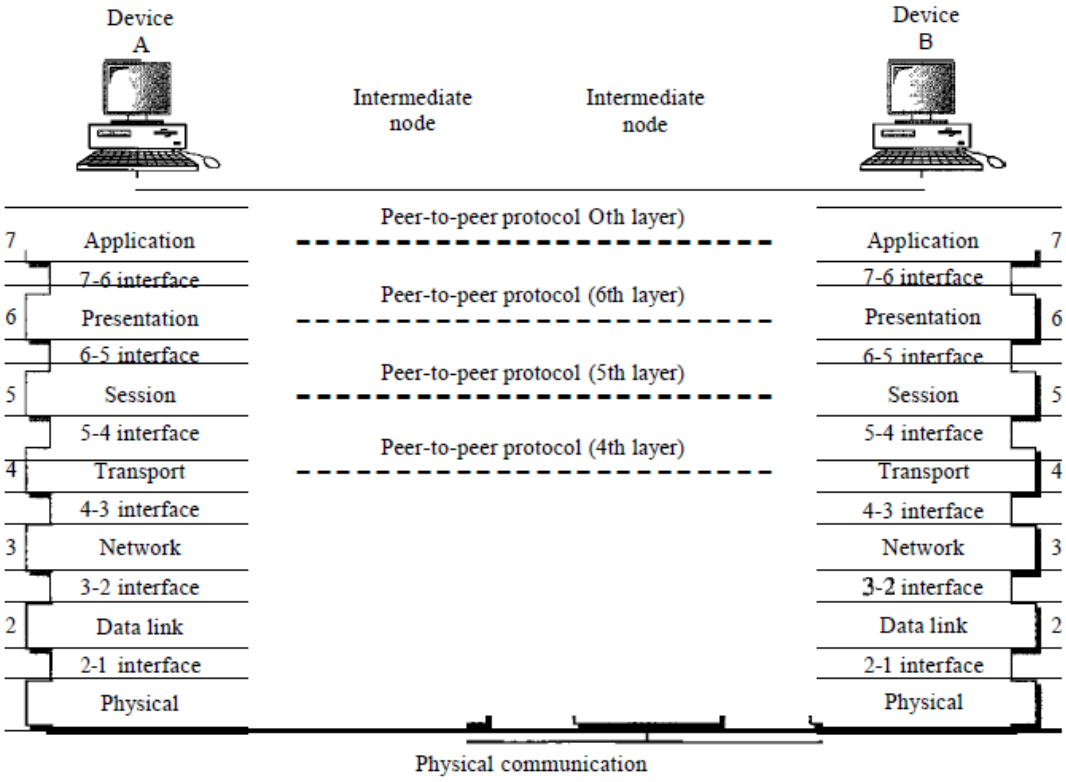
Encapsulation:

The process of adding overhead (header or trailer) to the PDU is called encapsulation

De-capsulation:

The process of removing overhead (header or trailer) to the PDU is called de-capsulation

LAYERS IN THE OSI MODEL



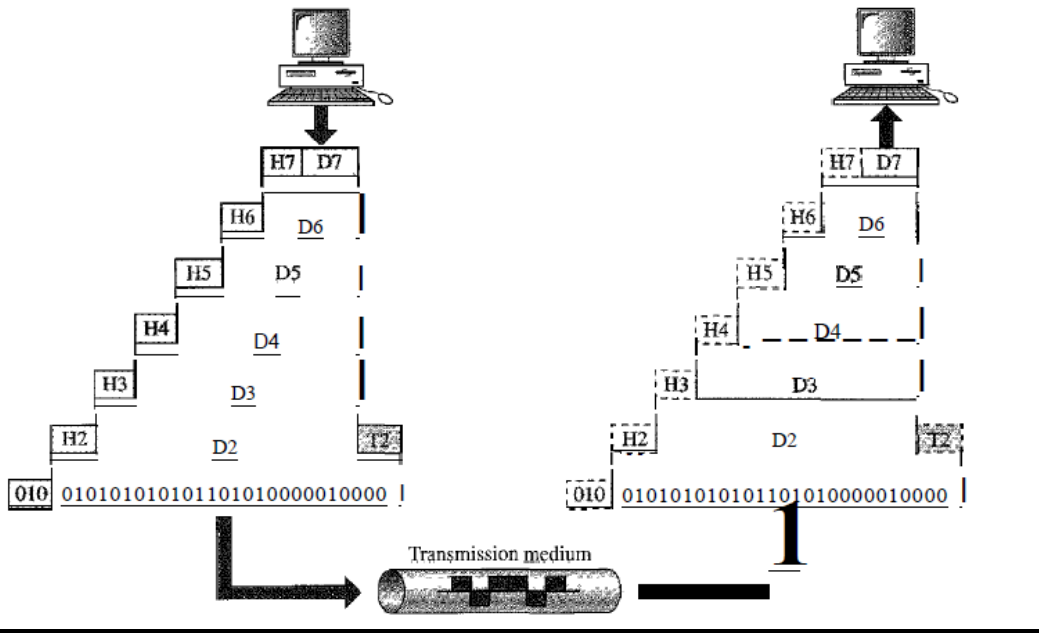


Figure: Exchange of data in OSI Model

The physical layer is also concerned with the following:

Transmission Media: Physical layer defines the type of transmission medium. Example wired (metallic cable, optical fiber cable), wireless (air, vacuum)

Representation of bits: The physical layer data consists of a stream of bits (sequence of Os or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how Os and I s are changed to signals).

Data rate: The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.

Synchronization of bits: The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.

Line configuration: The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.

Physical topology: The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology (every device is on a common link), or a hybrid topology (this is a combination of two or more topologies).

Transmission mode: The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex. In simplex mode, only one device can send; the other can only receive. The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

Data Link Layer

Framing:The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

Physical addressing(MAC Address): If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.

Flow control. If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

Error control: The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.

Access control: When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

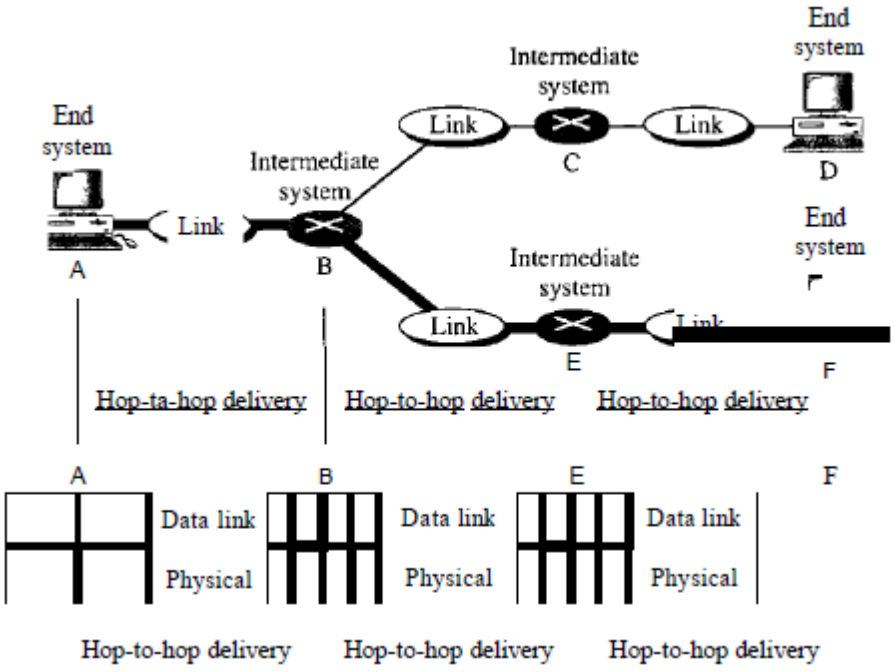


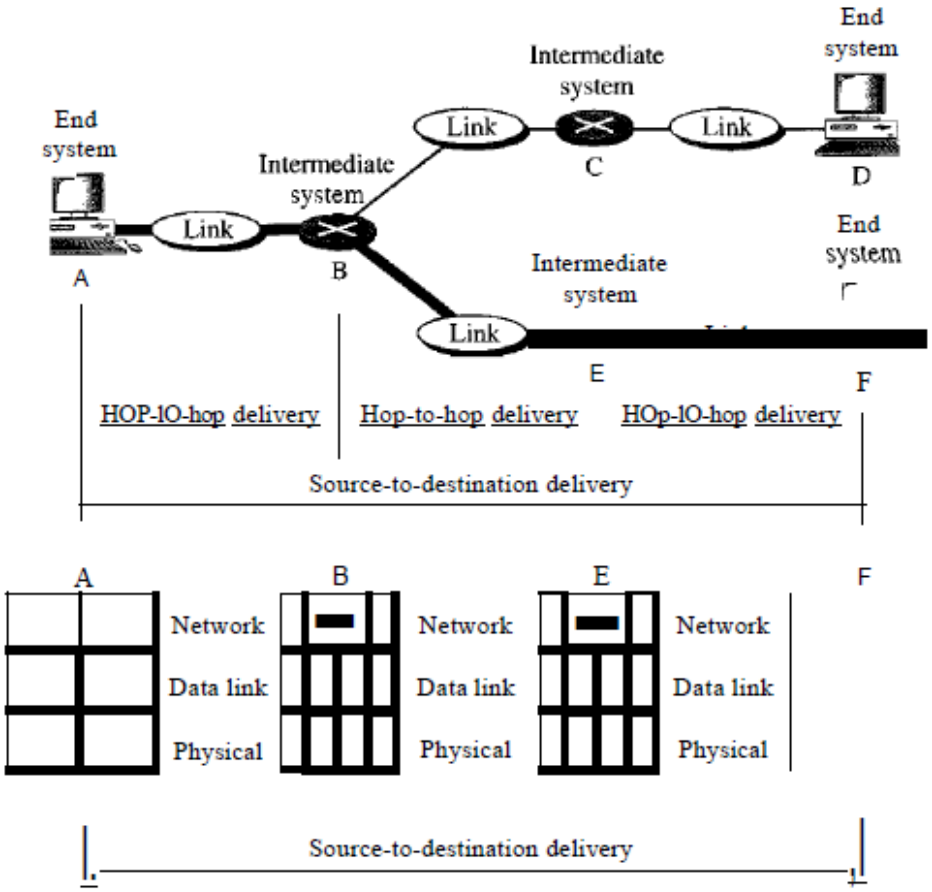
Figure: Hop to Hop delivery

Network Layer:

Logical addressing:The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary,we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver. We discuss logical addresses later in this chapter.

Routing: When independent networks or links are connected to create *intemetworks* (network of networks) or a large network, the connecting devices (called *routers* or *switches)* route or switch the packets to their final destination. One of the functions of the network layer is to provide this

mechanism.



Service-point addressing: Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a *service-point address* (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

Segmentation and reassembly: A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

Connection control: The transport layer can be either connectionless or connection-oriented.

A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented

transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.

Flow control. Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.

Error control. Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

Session layer:

A session is a temporary condition that exists when data are actually in the process of being transferred

Functions of Session layer are:

User authentication, network log on ,log off

Dialog control.: The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either halfduplex (one way at a time) or full-duplex (two ways at a time) mode.

Synchronization: The session layer allows a process to add checkpoints, or synChronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

Presentation Layer

Translation. The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The infonnation must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

Encryption. To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

Compression: Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

Application Layer:

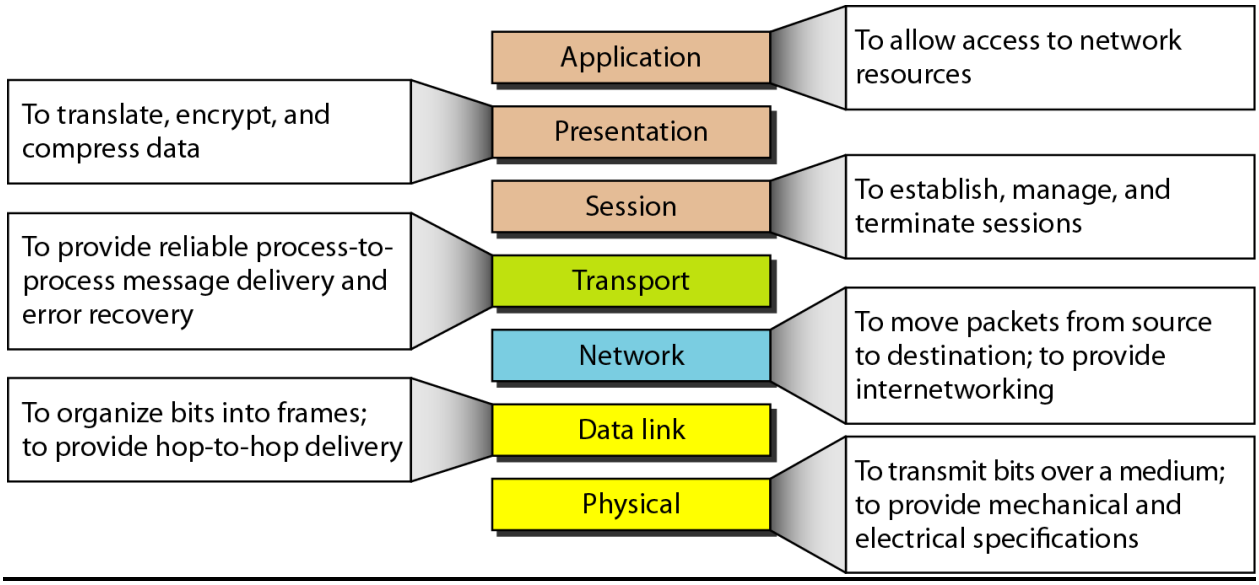
Remote Computer Access: Using TELNET protocol remote(far away) computers can be accessed

File transfer, access, and management. This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

Mail services. This application provides the basis for e-mail forwarding and storage.

Directory services. This application provides distributed database sources and access for global information about various objects and services

Summary of OSI Model



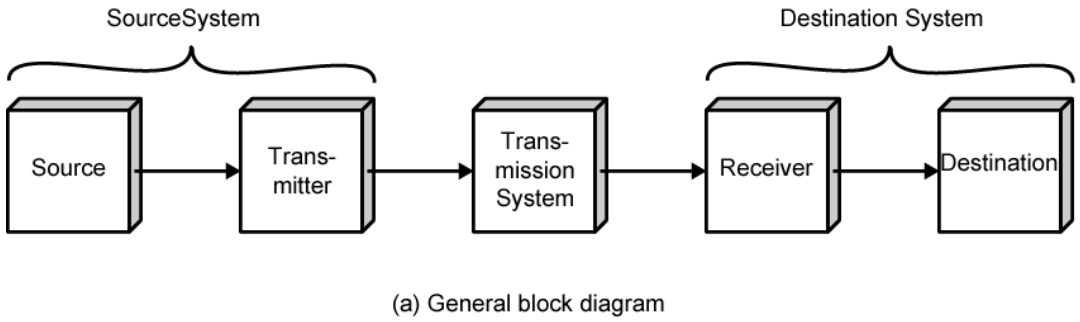
Data Communication Circuits

The underlying purpose of a digital communications circuit is to provide a transmission path between locations and to transfer digital information from one station (node, where computers or other digital equipment are located) to another using electronic circuits. Data communications circuits utilize

electronic communications equipment and facilities to interconnect digital computer equipment. Communication facilities are physical means of interconnecting stations and are provided to data communications users through public telephone networks (PTN), public data networks (PDN), and a multitude of private data communications systems.

The following figure shows a simple two-station data communications circuit. The main components are:

Source: - This device generates the data to be transmitted; examples are mainframe computer, personal computer, workstation etc. The source equipment provides a means for humans to enter data into system.



(a) General block diagram

(b) Example

Transmitter: - A transmitter transforms and encodes the information in such a way as to produce electromagnetic signals that can be transmitted across some sort of transmission system. For example, a modem takes a digital bit stream from an attached device such as a personal computer and transforms that bit stream into an analog signal that can be handled by the telephone network.

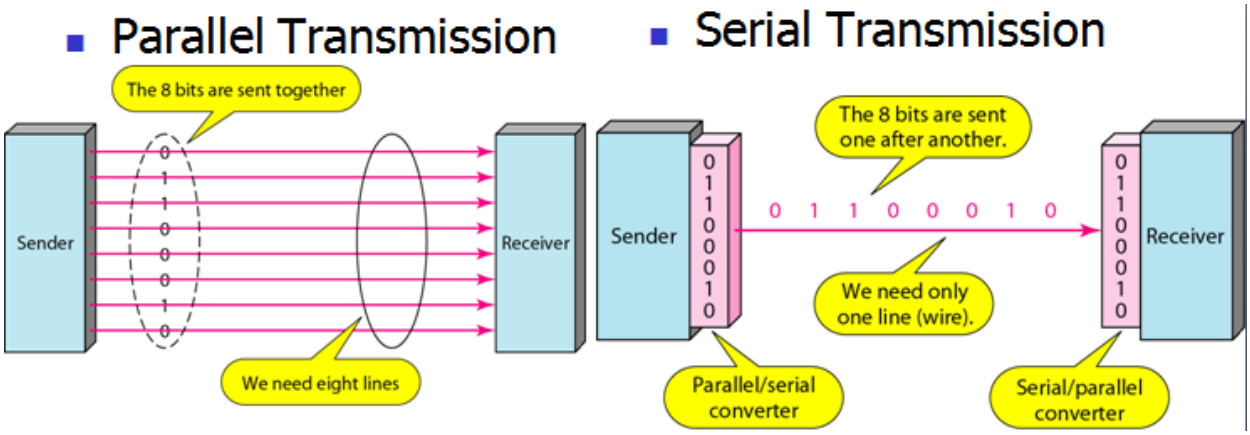
Transmission medium: - The transmission medium carries the encoded signals from the transmitter to the receiver. Different types of transmission media include free-space radio transmission (i.e. all forms of wireless transmission) and physical facilities such as metallic and optical fiber cables.

Receiver: - The receiver accepts the signal from the transmission medium and converts it into a form that can be handled by the destination device. For example, a modem will accept an analog signal coming from a network or transmission line and convert it into a digital bit stream.

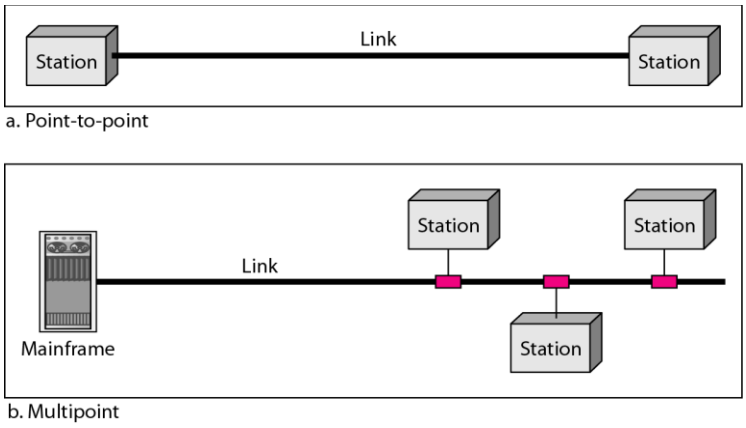
Destination: - Takes the incoming data from the receiver and can be any kind of digital equipment like the source.

Serial and Parallel Data Transmission

There are two methods of transmitting digital data namely ***parallel and serial*** transmissions. In parallel data transmission, all bits of the binary data are transmitted simultaneously. For example, to transmit an 8-bit binary number in parallel from one unit to another, eight transmission lines are required. Each bit requires its own separate data path. All bits of a word are transmitted at the same time. This method of transmission can move a significant amount of data in a given period of time. Its disadvantage is the large number of interconnecting cables between the two units. For large binary words, cabling becomes complex and expensive. This is particularly true if the distance between the two units is great. Long multiwire cables are not only expensive, but also require special interfacing to minimize noise and distortion problems. Serial data transmission is the process of transmitting binary words a bit at a time. Since the bits time-share the transmission medium, only one interconnecting lead is required.



While serial data transmission is much simpler and less expensive because of the use of a single interconnecting line, it is a very slow method of data transmission. Serial data transmission is useful in systems where high speed is not a requirement. Parallel communication is used for short-distance



data communications and within a computer, and serial transmission is used for long-distance data communications.

Data Communication Circuit Arrangements

A data communications circuit can be described in terms of circuit configuration and transmission mode.

Circuit Configurations Data communications networks can be generally categorized as either two point or multipoint. A *two-point* configuration involves only two locations or stations, whereas a *multipoint* configuration involves three or more stations.

A two-point circuit involves the transfer of digital information between a mainframe computer and a personal computer, two mainframe computers or two data communications networks. A multi-point network is generally used to interconnect a single mainframe computer (host) to many personal computers or to interconnect many personal computers and capacity of the channel is either *Spatially shared*: Devices can use the link simultaneously or *Timeshare*: Users take turns

Transmission Modes

There are four modes of transmission for data communications circuits:

In **simplex mode** the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive. Commercial radio broadcasting is an example. Simplex lines are also called receive-only, transmit-only or one-way-only lines. Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

In **half-duplex** mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

Example: Walkie-talkies, Citizens band (CB) radio is an example where push to talk (PTT) is to be pressed or depressed while sending and transmitting.

In **full-duplex mode** (called duplex), both stations can transmit and receive simultaneously. One common example of full-duplex communication is the telephone network. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel must be divided between the two directions.

In **full/full duplex** mode, transmission is possible in both directions at the same time but not between the same two stations (i.e. station 1 transmitting to station 2, while receiving from station 3). F/FDX is possible only on multipoint circuits. Postal system can be given as a person can be sending a letter to one address and receive a letter from another address at the same time.

Data Communications Networks

Any group of computers connected together can be called a *data communications network*, and the process of sharing resources between computers over a data communications network is called *networking*. The most important considerations of a data communications network are *performance, transmission rate, reliability and security.*

Network Components, Functions, and Features

The major components of a network are end stations, applications and a network that will support traffic between the end stations. Computer networks all share common devices, functions, and features, including servers, clients, transmission media, shared data, shared printers and other peripherals, hardware and software resources, network interface card (NIC), local operating system (LOS) and the network operating system (NOS).

Servers: Servers are computers that hold shared files, programs and the network operating system. Servers provide access to network resources to all the users of the network and different kinds of

servers are present. Examples include file servers, print servers, mail servers, communication servers etc.

Clients: Clients are computers that access and use the network and shared network resources. Client computers are basically the customers (users) of the network, as they request and receive service from the servers.

Shared Data: Shared data are data that file servers provide to clients, such as data files, printer access programs, and e-mail.

Shared Printers and other peripherals: these are hardware resources provided to the users of the network by servers. Resources provided include data files, printers, software, or any other items used by the clients on the network.

Network interface card: Every computer in the network has a special expansion card called network interface card (NIS), which prepares and sends data, receives data, and controls data flow between the computer and the network. While transmitting, NIC passes frames of data on to the physical layer and on the receiver side, the NIC processes bits received from the physical layer and processes the message based on its contents.

Local operating system: A local operating system allows personal computers to access files, print to a local printer, and have and use one or more disk and CD drives that are located on the computer. Examples are MS-DOS, PC-DOS, UNIX, Macintosh, OS/2, Windows 95, 98, XP and Linux.

Network operating system: the NOS is a program that runs on computers and servers that allows the computers to communicate over a network. The NOS provides services to clients such as log-in features, password authentication, printer access, network administration functions and data file sharing.

Network Models

Computer networks can be represented with two basic network models: peer-to-peer client/server and dedicated client/server. The client/server method specifies the way in which two computers can communicate with software over a network.

Peer-to-peer client/server network: Here, all the computers share their resources, such as hard drives, printers and so on with all the other computers on the network. Individual resources like disk

drives, CD-ROM drives, and even printers are transformed into shared, collective resources that are accessible from every PC. Unlike client-server networks, where network information is stored on a centralized file server PC and made available to tens, hundreds, or thousands client PCs, the information stored across peer-to-peer networks is uniquely decentralized. Because peer-to-peer PCs have their own hard disk drives that are accessible by all computers, each PC acts as both a client (information requestor) and a server (information provider). The peer-to-peer network is an appropriate choice when there are fewer than 10 users on the network, security is not an issue and all the users are located in the same general area.

The advantages of peer-to-peer over client-server NOSs include:

- No need for a network administrator
- Network is fast/inexpensive to setup & maintain
- Each PC can make backup copies of its data to other PCs for security.
- Easiest type of network to build, peer-to-peer is perfect for both home and office use.

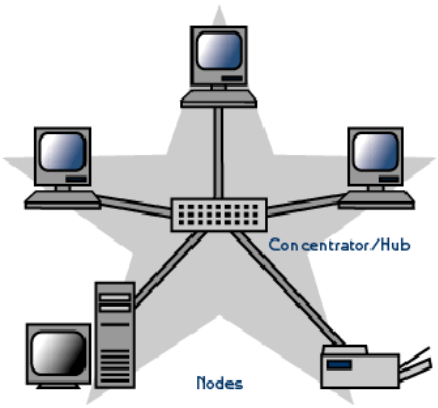
Dedicated client/server network: Here, one computer is designated as server and the rest of the computers are clients. Dedicated Server Architecture can improve the efficiency of client server systems by using one server for each application that exists within an organization. The designated servers store all the networks shared files and applications programs and function only as servers and are not used as a client or workstation. Client computers can access the servers and have shared files transferred to them over the transmission medium. In some client/server networks, client computers submit jobs to one of the servers and once they process the jobs, the results are sent back to the client computer. In general, the dedicated client/server model is preferable to the peer-to-peer client/server model for general purpose data networks.

Network Topologies

In computer networking, *topology* refers to the layout of connected devices, i.e. how the computers, cables, and other components within a data communications network are interconnected, both physically and logically. The physical topology describes how the network is actually laid out, and the logical topology describes how the data actually flow through the network. Two most basic

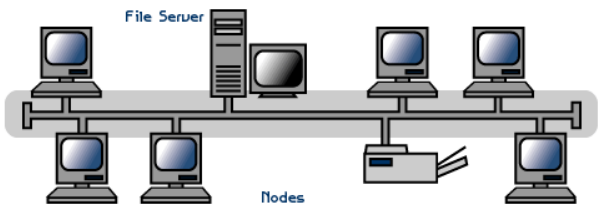
topologies are point-to-point and multipoint. A point-to-point topology usually connects two mainframe computers for high-speed digital information. A multipoint topology connects three or more stations through a single transmission medium and some examples are *star, bus, ring, mesh and hybrid.*

Star topology: A star topology is designed with each node (file server, workstations, and peripherals) connected directly to a central network hub, switch, or concentrator. Data on a star network passes through the hub, switch, or concentrator before continuing to its destination. The hub, switch, or concentrator manages and controls all functions of the network. It also acts as a repeater for the data flow.



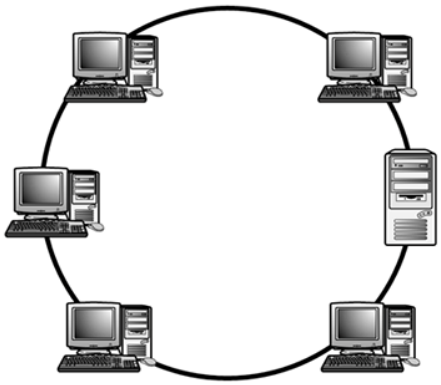
Advantages	Disadvantages
Easily expanded without disruption to the network	Requires more cable
Cable failure affects only a single user	A central connecting device allows for a single point of failure
Easy to troubleshoot and isolate problems	More difficult to implement

Bus topology: Bus networks use a common backbone to connect all devices. A single cable, (the backbone) functions as a shared communication medium that devices attach or tap into with an interface connector. A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message. The bus topology is the simplest and most common method of interconnecting computers. The two ends of the transmission line never touch to form a complete loop. A bus topology is also known as multi-drop or linear bus or a horizontal bus.



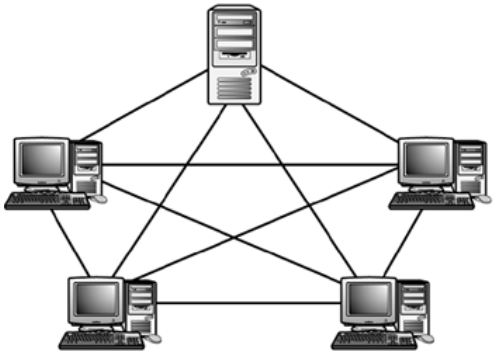
Advantages	**Disadvantages**
Cheap and easy to implement	Network disruption when computers are added or removed
Require less cable	A break in the cable will prevent all systems from accessing the network.
Does not use any specialized network equipment.	Difficult to troubleshoot.

Ring topology: In a ring network (sometimes called a loop), every device has exactly two neighbours for communication purposes. All messages travel through a ring in the same direction (either "clockwise" or "counter clockwise"). All the stations are interconnected in tandem (series) to form a closed loop or circle. Transmissions are unidirectional and must propagate through all the stations in the loop. Each computer acts like a repeater and the ring topology is similar to bus or star topologies



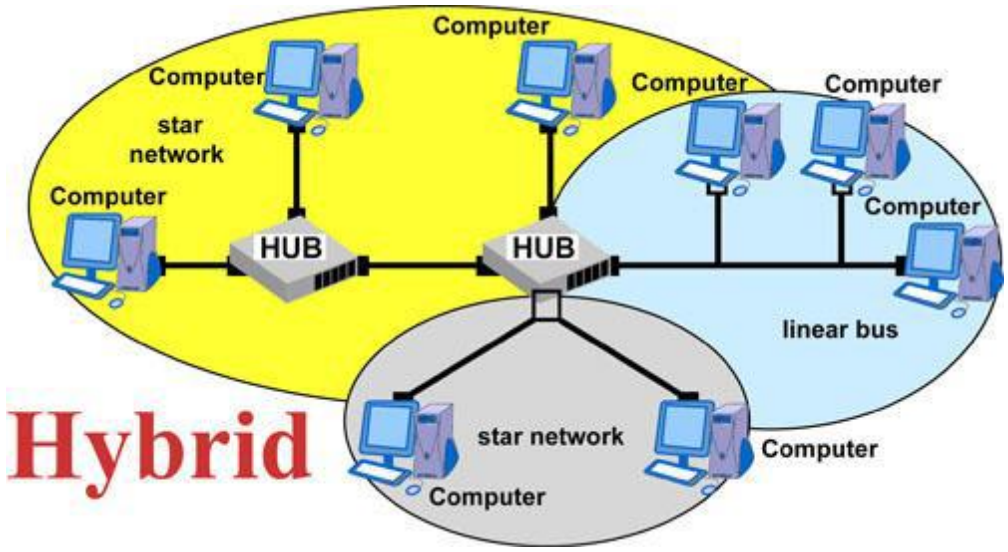
Advantages	Disadvantages
Cable faults are easily located, making troubleshooting easier	Expansion to the network can cause network disruption
Ring networks are moderately easy to install	A single break in the cable can disrupt the entire network.

Mesh topology: The *mesh* topology incorporates a unique network design in which each computer on the network connects to every other, creating a point-to-point connection between every device on the network. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. A mesh network in which every device connects to every other is called a full mesh. A disadvantage is that, a mesh network with *n* nodes must have *n(n-1)/2* links and each node must have *n-1* I/O ports (links).



Advantages	Disadvantages
Provides redundant paths between devices	Requires more cable than the other LAN topologies
The network can be expanded without disruption to current uses	Complicated implementation

Hybrid topology: This topology (sometimes called mixed topology) is simply combining two or more of the traditional topologies to form a larger, more complex topology. Main aim is being able to share the advantages of different topologies.



Network Classifications

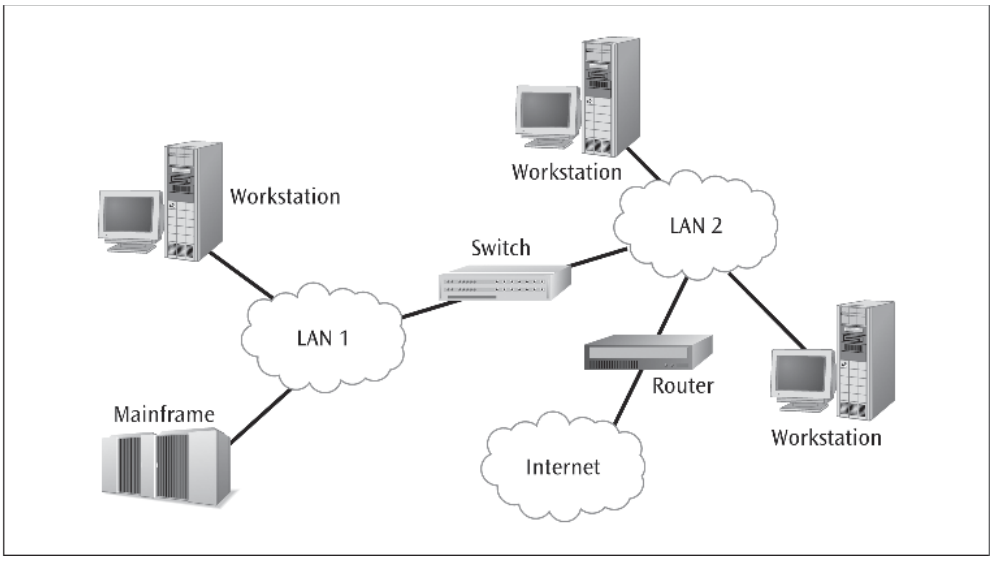
One way to categorize the different types of computer network designs is by their scope or scale. Common examples of area network types are:

- LAN - Local Area Network
- WLAN - Wireless Local Area Network
- WAN - Wide Area Network
- MAN - Metropolitan Area Network
- GAN - Global Area Network
- PAN - Personal Area Network
- PLAN - Power line area Network

Local area network:

A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings. LANs use a network operating system to provide two-way communications at bit rates in the range of 10 Mbps to 100 Mbps. In addition to operating in a limited space, LANs are also typically owned, controlled, and managed by a single person or organization. They also tend to use certain connectivity technologies, primarily Ethernet and Token Ring.

Figure 7-1
A local area network interconnecting another local area network, the Internet, and a mainframe computer



Advantages of LAN:

- Share resources efficiently
- Individual workstation might survive network failure if it doesn't rely upon others
- Component evolution independent of system evolution
- Support heterogeneous hardware/software
- Access to other LANs and WANs
- High transfer rates with low error rates

Metropolitan area network:

A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities. Its geographic scope falls between a WAN and LAN. A MAN might be a single network like the cable television network or it usually interconnects a number of local area networks (LANs) using a high-capacity backbone technology, such as fiber-optical links, and provides up-link services to wide area networks and the Internet. MANs typically operate at speeds of 1.5 Mbps to 10 Mbps and range from five miles to a few hundred miles in length. Examples of MANs are FDDI (fiber distributed data interface) and ATM (asynchronous transfer mode).

Wide area network: Wide area networks are the oldest type of data communications network that provide relatively slow-speed, long-distance transmission of data, voice and video information over relatively large and widely dispersed geographical areas, such as country or entire continent. WANs interconnect routers in different locations. A WAN differs from a LAN in several important ways.

Most WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management. WANs tend to use technology like ATM, Frame Relay and X.25 for connectivity over the longer distances.

Global area network: A GAN provides connections between countries around the entire globe. Internet is a good example and is essentially a network comprised of other networks that interconnect virtually every country in the world. GANs operate from 1.5 Mbps to 100 Gbps and cover thousands of miles.

Campus Area Network: - a network spanning multiple LANs but smaller than a MAN, such as on a university or local business campus.

Storage Area Network: - connects servers to data storage devices through a technology like Fibre Channel.

System Area Network: - Links high-performance computers with high-speed connections in a cluster configuration. Also known as Cluster Area Network.

Building backbone: - It is a network connection that normally carries traffic between departmental LANs within a single company. It consists of a switch or router to provide connectivity to other networks such as campus backbones, enterprise backbones, MANs, WANs etc

Camus backbone: - **It** is a network connection used to carry traffic to and from LANs located in various buildings on campus. It normally uses optical fiber cables for the transmission media between buildings and operates at relatively high transmission rates.

Enterprise networks: - It includes some or all of the above networks and components connected in a cohesive and manageable fashion.

Alternate Protocol Suites

The protocols other than OSI that are in wide spread used are TCP?IP and the Cisco three-layer hierarchical model.

TCP/IP Protocol Suite

The TCPIIP protocol suite was developed prior to the OSI model. Therefore, the layers

in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers:

- **Host-to-network Layer**
- **Internet Layer**
- **Transport Layer**
- **Application Layer**

However, when TCP/IP is compared to OSI, we can say that the

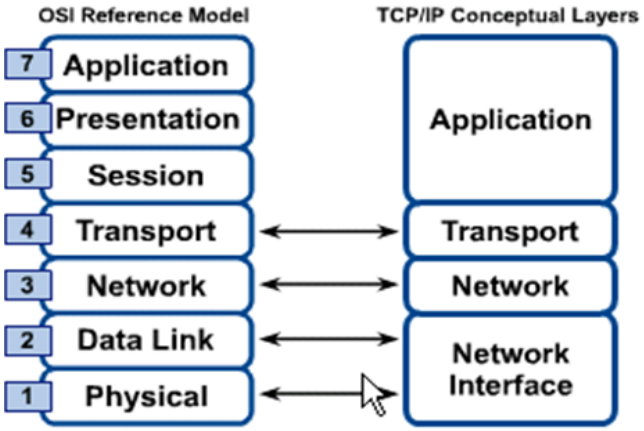
Host-to-network layer .It is also called **network access layer** .It is equivalent to the combination of the physical and data link layers.

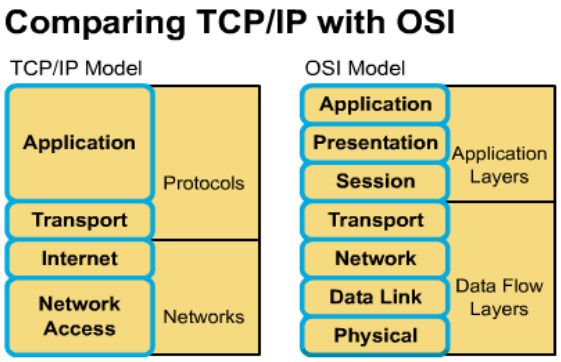
Internet layer is equivalent to the network layer The purpose of the ***Internet layer*** is to send source packets from any network on the internetwork and have them arrive at the destination independent of the path and networks they took to get there. The specific protocol that governs this layer is called the **Internet protocol** (IP). *Best path determination* and *packet switching* occur at this layer.

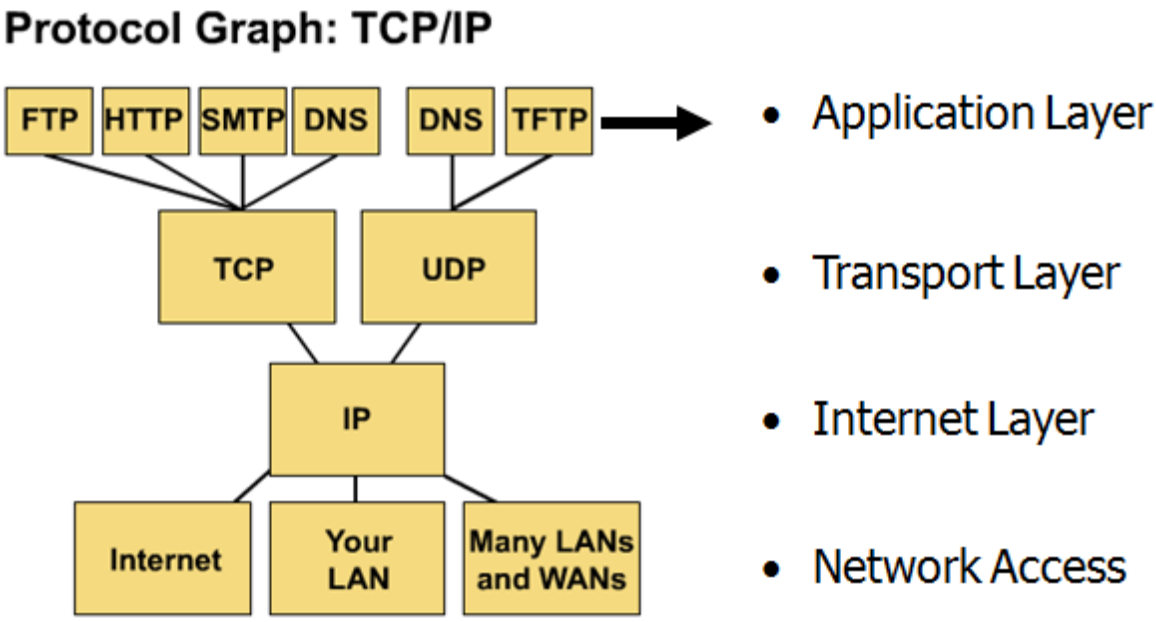
Transport layer of the TCP/IP deals with the quality-of-service issues of reliability, flow control, and error correction. One of its protocols, the transmission control protocol (TCP), provides excellent and flexible ways to create reliable, well-flowing, low-error network communications. TCP is a ***connection-oriented protocol*.** The other protocol is User Datagram Protocol (UDP) which is a **connection less protocol**.

Application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCP/IP taking care of part of the duties of the session layer.

The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the *application layer*.







Differences between OSI and TCP/IP

- TCP/IP combines the presentation and session layer issues into its application layer
- TCP/IP combines the OSI data link and physical layers into one layer
- TCP/IP appears simpler because it has fewer layers
- TCP/IP protocols are the standards around which the Internet developed, so the TCP/IP model gains credibility just because of its protocols. In contrast, typically networks aren't built on the OSI protocol, even though the OSI model is used as a guide.

Cisco Three Layer Model

- Cisco has defined a hierarchical model known as the hierarchical internetworking model. This model simplifies the task of building a reliable, scalable, and less expensive hierarchical internetwork because rather than focusing on packet construction; it focuses on the three functional areas, or layers, of your network.
- **Core layer**: This layer is considered the backbone of the network and includes the high-end switches and high-speed cables such as fiber cables. This layer of the network does not route traffic at the LAN. In addition, no packet manipulation is done by devices in this layer. Rather, this layer is concerned with speed and ensures reliable delivery of packets.
- **Distribution layer**: This layer includes LAN-based routers and layer 3 switches. This layer ensures that packets are properly routed between subnets and VLANs in your enterprise. This layer is also called the Workgroup layer. It also provides policy-based network connectivity, including:
- **Packet filtering (firewalling)**: Processes packets and regulates the transmission of packets based on its source and destination information to create network borders.
- **QoS**: The router or layer 3 switches can read packets and prioritize delivery, based on policies set.
- **Access Layer Aggregation Point**: The layer serves the aggregation point for the desktop layer switches.
- **Control Broadcast and Multicast**: The layer serves as the boundary for broadcast and multicast domains.
- **Application Gateways**: The layer allows you to create protocol gateways to and from different network architectures.
- The distribution layer also performs queuing and provides packet manipulation of the network traffic.

Access layer: This layer includes hubs and switches. This layer is also called the desktop layer because it focuses on connecting client nodes, such as workstations to the network. This layer ensures that packets are delivered to end user computers. At the access layer, you can:

- **Enable MAC address filtering**: It is possible to program a switch to allow only certain systems to access the connected LANs.

- **Create separate collision domains**: A switch can create separate collision domains for each connected node to improve performance.
- **Share bandwidth**: You can allow the same network connection to handle all data.
- **Handle switch bandwidth**: You can move data from one network to another to perform load balancing.

The benefits of the Cisco hierarchical model includes:

- **High Performance**: You can design high performance networks, where only certain layers are susceptible to congestion.
- **Efficient management & troubleshooting**: Allows you to efficiently organize network management and isolate causes of network trouble.
- **Policy creation**: You can easily create policies and specify filters and rules.
- **Scalability**: You can grow the network easily by dividing your network into functional areas.
- **Behavior prediction**: When planning or managing a network, the model allows you determine what will happen to the network when new stresses are placed on it.