Unit – 5: Data Communication and Computer Network

Contents: Introduction to Communication system, Modes of Communication, Introduction to Computer Network, LAN Topologies, Transmission Media, Network Devices, OSI Reference Model, Communication Protocols, Centralized vs Distributed System

Introduction to Data Communication

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

Fundamental Characteristics

The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. Delivery

   The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

2. Accuracy.

   The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable

3. Timeliness.

   The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

4. Jitter

   Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets

Components of Data Communication

A data communications system has five components

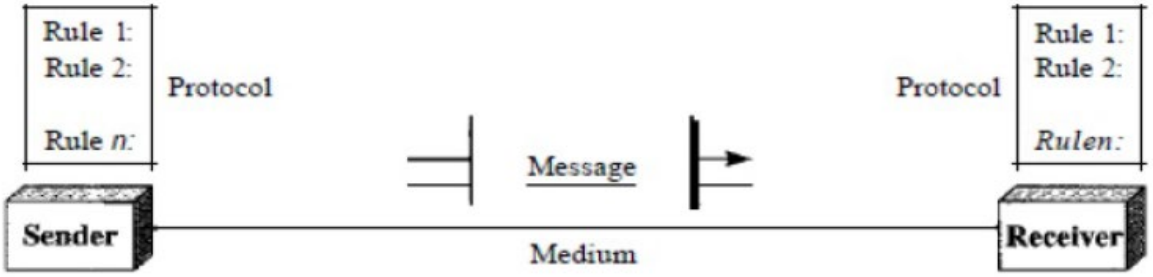


Fig: Components of Data Communication

1. Message

   The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

2. Sender

   The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3. Receiver

   The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4. Transmission medium

   The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

5. Protocol

   A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.

Mode of Data Communication

Communication between two devices can be simplex, half-duplex, or full-duplex

Simplex:

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. 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.

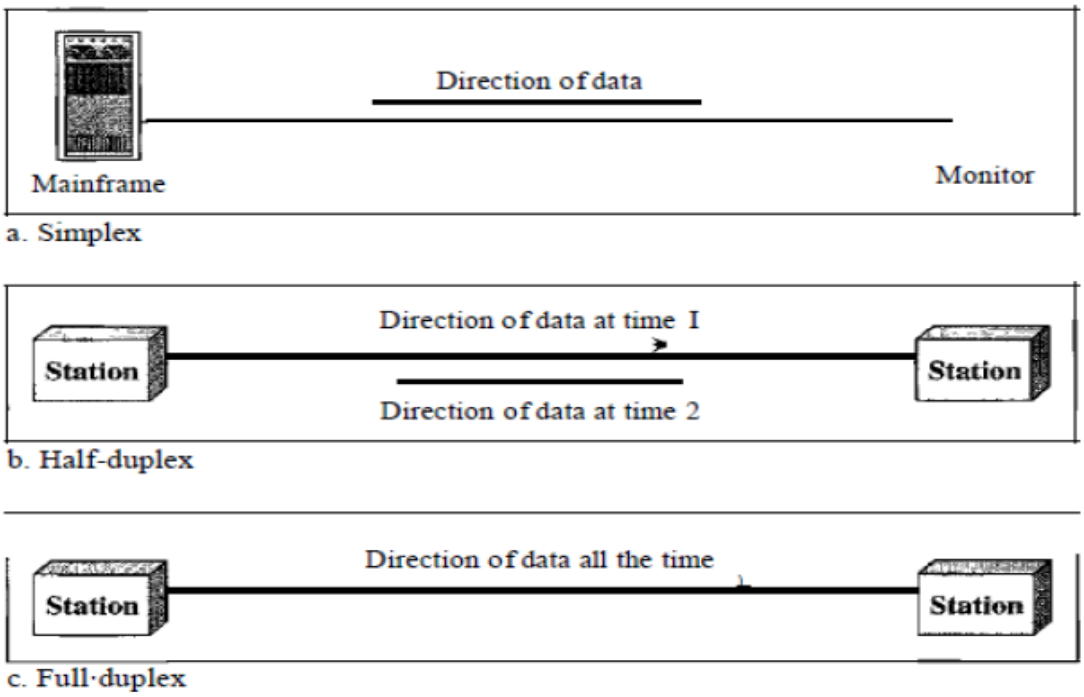
Half-Duplex:

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. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems. 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

Full-Duplex:

In full-duplex both stations can transmit and receive simultaneously. The full-duplex mode is like a two way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction. One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

Data Flow in different modes



Computer Network

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users.

Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security

1. Performance:

   Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

2. Reliability:

   Network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

3. Security:

   Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Types of Connections

There are two types of connections.

1. Point-to-Point

   A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices.

2. Multipoint

   A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link.

   In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

Types of Computer Network

Networks may be divided into different types and categories according to four different criteria

1. Geographic spread of nodes and hosts

   When the physical distance between the hosts is within a few kilometers, the network is said to be a Local area Network (LAN). LANs are typically used to connect a set of hosts within the same building (e.g., an office environment) or a set of closely-located buildings (e.g., a university campus)

   For larger distances, the network is said to be a Metropolitan Area Network (MAN) or a Wide Area Network (WAN). MANs cover distances of up to a few hundred kilometers and are used for interconnecting hosts spread across a city.

   WANs are used to connect hosts spread across a country, a continent, or the globe

2. Access restrictions

   Most networks are for the private use of the organizations to which they belong; these are called private networks. Networks maintained by banks, insurance companies, airlines, hospitals, and most other businesses are of this nature

   Public networks, on the other hand, are generally accessible to the average user, but may require registration and payment of connection fees. Internet is the most-widely known example of a public network.

3. Communication model employed by the nodes

   The communication between the nodes is either based on a point-to-point model or a broadcast model.

4. Switching model employed by the nodes

   In the point-to-point model, nodes either employ circuit switching or packet switching. In circuit switching, a dedicated communication path is allocated between A and B, via a set of intermediate nodes. In packet switching, data is divided into packets (chunks of specific length and characteristics) which are sent from A to B via intermediate nodes. Each intermediate node temporarily stores the packet and waits for the receiving node to become available to receive it

LAN Topologies

Various topologies are possible for the broadcast LAN such as bus, ring or mesh topology.

1. BUS Topology

   A bus topology is multipoint. One long cable act as a backbone to link all the devices in a network. Nodes are connected to the bus cable by drop lines and taps.

   As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason, there is a limit on the number of taps a bus can support and on the distance between those taps.

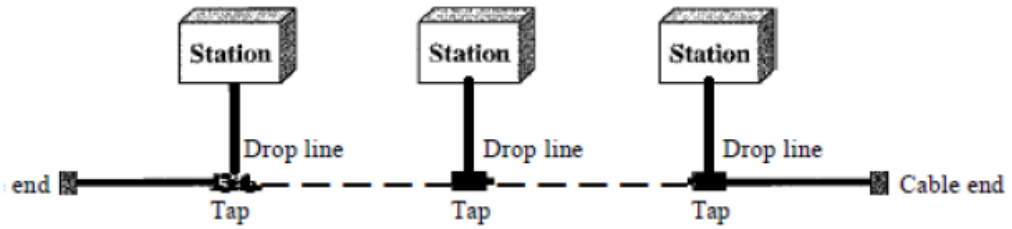


Fig: Bus Topology

2. Ring Topology

   In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

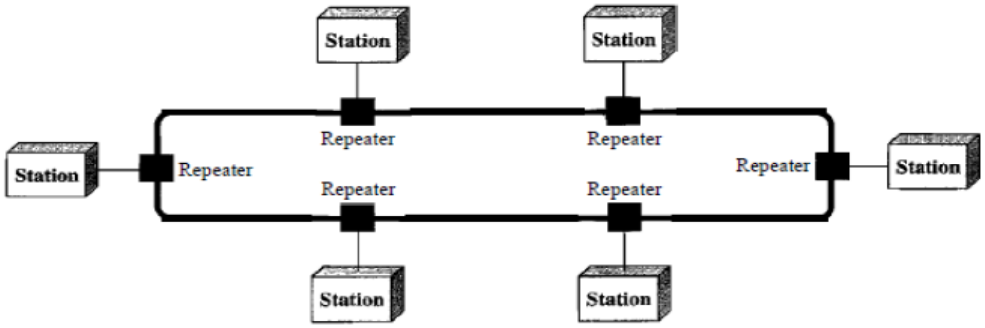


Fig: Ring Topology

3. Star Topology:

   In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an

exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

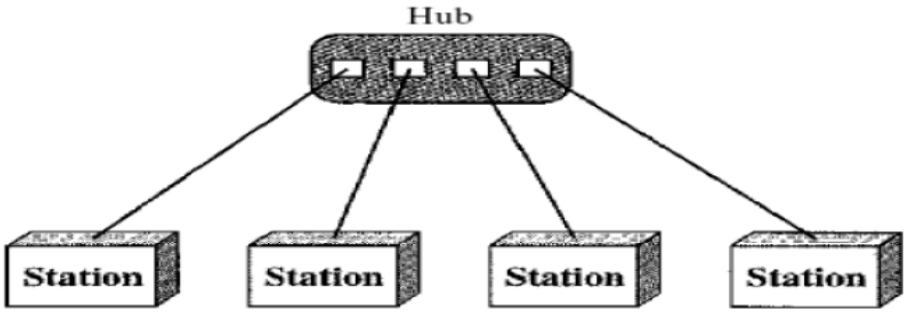


Fig: Star Topology

4. Mesh Topology

   In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects.

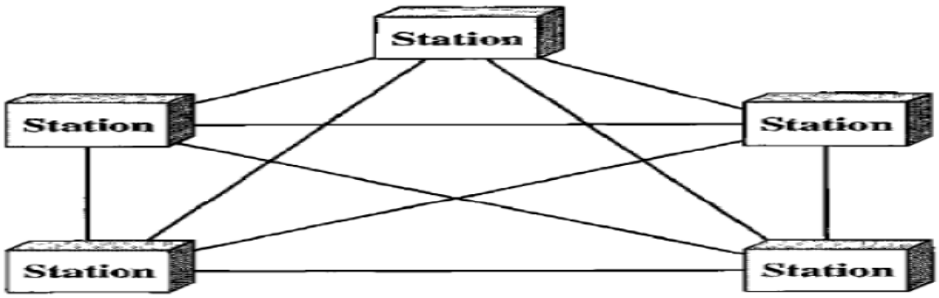


Fig: Mess Topology

Transmission Media

A transmission medium can be broadly defined as anything that can carry information from a source to a destination. The transmission medium is usually free space, metallic cable, or fiber-optic cable. The information is usually a signal that is the result of a conversion of data from another form.

Guided Media

A signal traveling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

1. Twisted-Pair Cable

   A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together. One of the wires is used to carry signals to the receiver, and the other is used

only as a ground reference. The signal sent by the sender on one of the wires causes interference (noise) and crosstalk creating unwanted signals. Twisting the pair of cable reduces interference and cross talk between signals. For example, Twisted-pair cables are used in telephone lines to provide voice and data channels.

2. Coaxial Cable

   Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two.

3. Fiber Optic Cable:

   A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. To understand optical fiber, we first need to explore several aspects of the nature of light. Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.

   Advantages

   - Higher bandwidth. Fiber-optic cable can support dramatically higher bandwidths
   - Less signal attenuation. Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration.
   - Immunity to electromagnetic interference. Electromagnetic noise cannot affect fiber-optic cables.
   - Resistance to corrosive materials. Glass is more resistant to corrosive materials than copper.
   - Light weight. Fiber-optic cables are much lighter than copper cables.
   - Greater immunity to tapping. Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

   Disadvantages

   - Installation and maintenance is difficult
   - Unidirectional light propagation. Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.

UNGUIDED MEDIA: WIRELESS

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation

Network device

1. Repeaters

   A repeater is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data. A repeater receives a signal and, before it becomes too weak or corrupted, regenerates the original bit pattern. A repeater does not actually connect two LANs; it connects two segments of the same LAN.

2. Bridges or Link Layer Switches

   A bridge or Link layer switch (or simply Switch) operates in both the physical and the data link layer. As a physical layer device, it regenerates the signal it receives. As a data link layer device, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame. A bridge has filtering capability. A bridge has a table that maps addresses to ports.

3. Hubs

   A Hub is a device that operates only in the physical layer. It is basically used for connecting stations in a physical star topology. The main disadvantage of Hub is that it broadcast data to all the devices connected to it. So, chances of collision and data corruption is high in hubs.

4. Routers

   A router is a three-layer device that routes packets based on their logical addresses (host-to-host addressing). A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route. The routing tables are normally dynamic and are updated using routing protocols.

   There are three major differences between a router and a repeater or switch.

   - A router has a physical and logical address for each of its interfaces.
   - A router acts only on those packets in which the link layer destination address matches the address of the interface at which the packet arrives.
   - A router changes the link layer address of the packet when it forwards the packet

5. Gateway

   A gateway is normally a computer that operates in all five layers of the Internet or seven layers of OSI model. A gateway takes an application message, reads it, and interprets it. This means that it can be used as a connecting device between two internetworks that use different models

OSI Reference Model

The model is called the ISO-OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems.

The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.

The OSI model is composed of seven ordered layers: physical (layer 1), data link (layer 2), network (layer 3), transport (layer 4), session (layer 5), presentation (layer 6), and application (layer 7).

As the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model

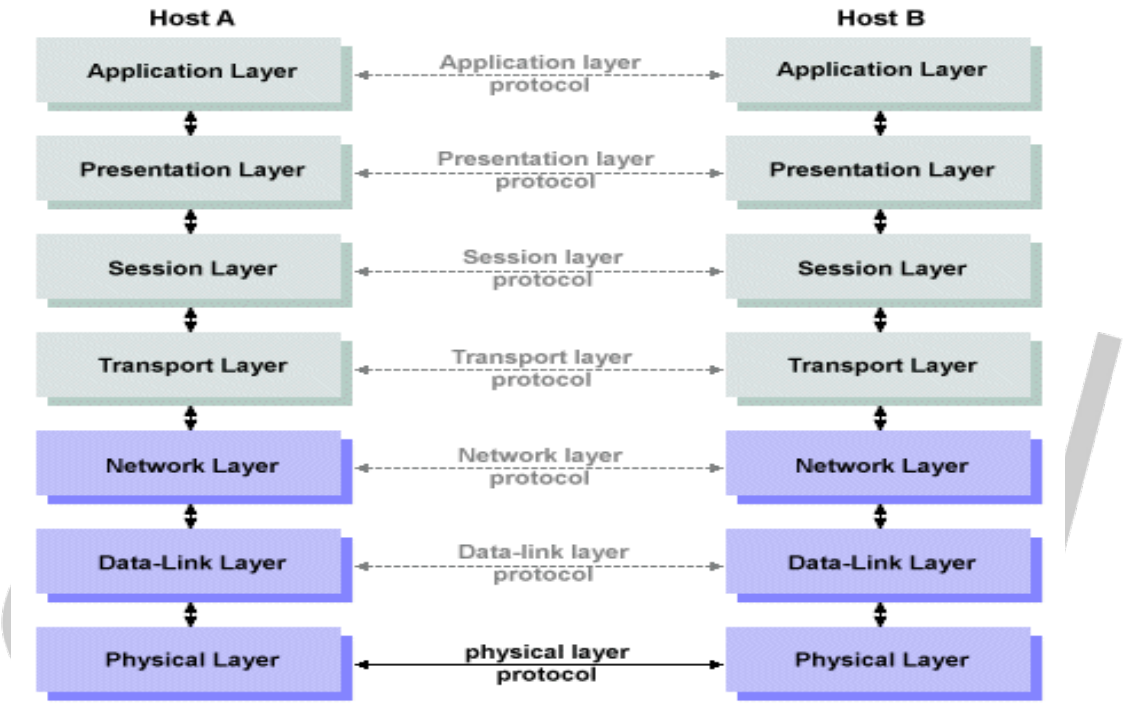


Fig: OSI-ISO Reference Model

Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also

defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.

Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer).

Other responsibilities of the data link layer include the following

- **Framing** - The data link layer divides the stream of bits received from the network layer into manageable data units called frames
- Physical addressing
- **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

Network Layer

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

Other responsibilities of the network layer include the following:

- **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.
- **Routing** - When independent networks or links are connected to create internetworks (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.

Transport Layer

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does.

The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

Other function includes

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

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems.

Specific responsibilities of the session layer include the following:

- **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 half duplex (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

Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems

- **Translation** - 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

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

Specific services provided by the application layer include the following:

- **Network virtual terminal** - A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
- **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.

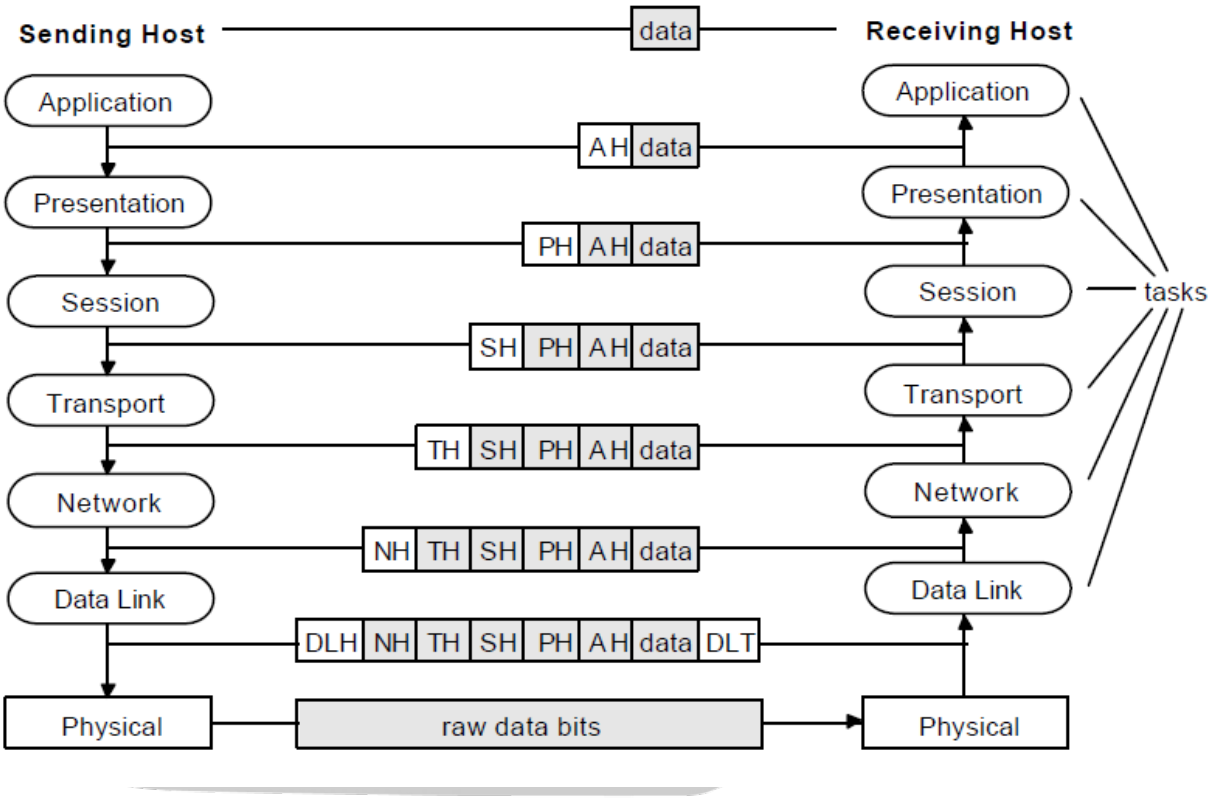


Fig: OSI Layers as Software tasks

Communication Protocols

All communications between devices require that the devices agree on the format of the data. The set of rules defining a format is called a protocol. At the very least, a communications protocol must define the following:

- rate of transmission (in baud or bps)
- whether transmission is to be synchronous or asynchronous
- whether data is to be transmitted in half-duplex or full-duplex mode

In addition, protocols can include sophisticated techniques for detecting and recovering from transmission errors and for encoding and decoding data.

Centralized vs Decentralized System

Distributed System

A distributed system is a collection of independent computers that appear to the users of the system as a single system. A Distributed system consists of multiple autonomous computers, each having its own private memory, communicating through a computer network. Information exchange in a distributed system is accomplished through message passing.

Examples

- World Wide Web (WWW) is the biggest example of distributed system.
- The internet
- An intranet which is a portion of the internet managed by an organization
- Network of branch office computers

Advantages of Distributed Systems over Centralized Systems

- **Economics** - A collection of microprocessors offers a better price/performance than mainframes. Low price/performance ratio: cost effective way to increase computing power.
- **Speed** - A distributed system may have more total computing power than a mainframe. Ex. 10,000 CPU chips, each running at 50 MIPS. Not possible to build 500,000 MIPS single processor since it would require 0.002 sec instruction cycle. Enhanced performance through load distributing.
- **Inherent distribution** - Some applications are inherently distributed. Ex. a supermarket chain.
- **Reliability** - If one machine crashes, the system as a whole can still survive. Higher availability and improved reliability.
- **Incremental growth** - Computing power can be added in small increments. Modular expand-ability
- **Another deriving force** - The existence of large number of personal computers, the need for people to collaborate and share information.
- **Open system** - This is the most important point and the most characteristic point of a distributed system. Since it is an open system it is always ready to communicate with other

systems. An open system that scales has an advantage over a perfectly closed and self-contained system.