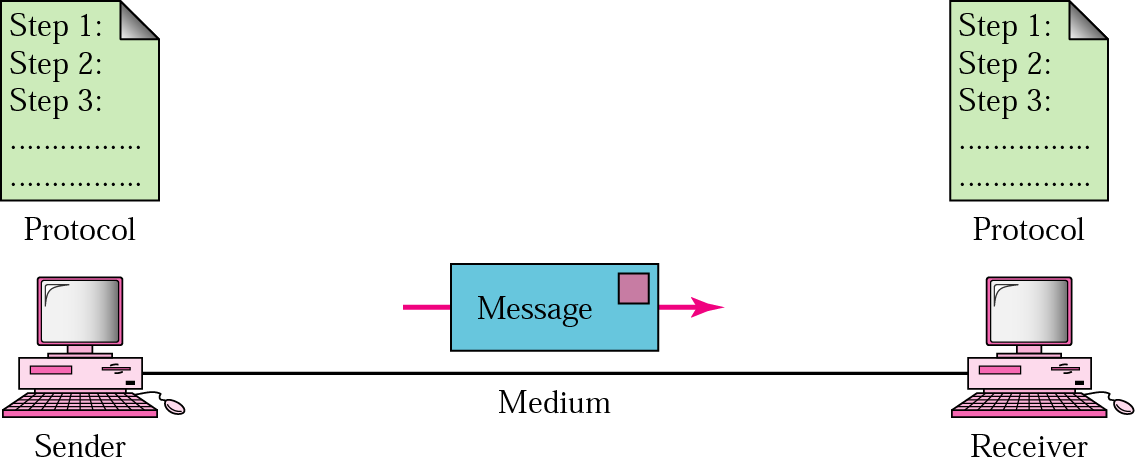
**Q. Explain the components of Data Communication.**

**Fig:** Components of Data Communication

**Protocol:** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

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

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

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

**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

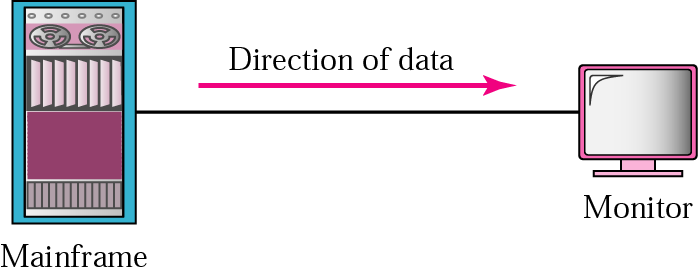
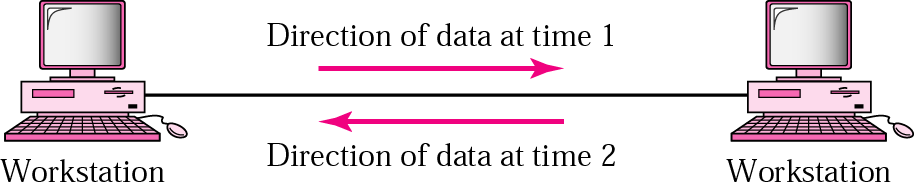
**Q. What is Data Flow? Explain different modes of Data Flow.**

Fig: Simplex Mode

In simplex mode, the communication is unidirectional, as on a one-way street. Only one ofthe two devices on a link can transmit; the other can only receive (see Figure 1.2a). 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 ofthe channel to send data in one direction.

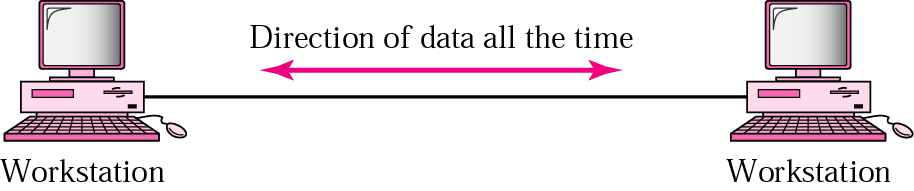
**Half-Duplex**

****

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.

The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait. 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 ofthe channel can be utilized for each direction.

**Full-Duplex**

****

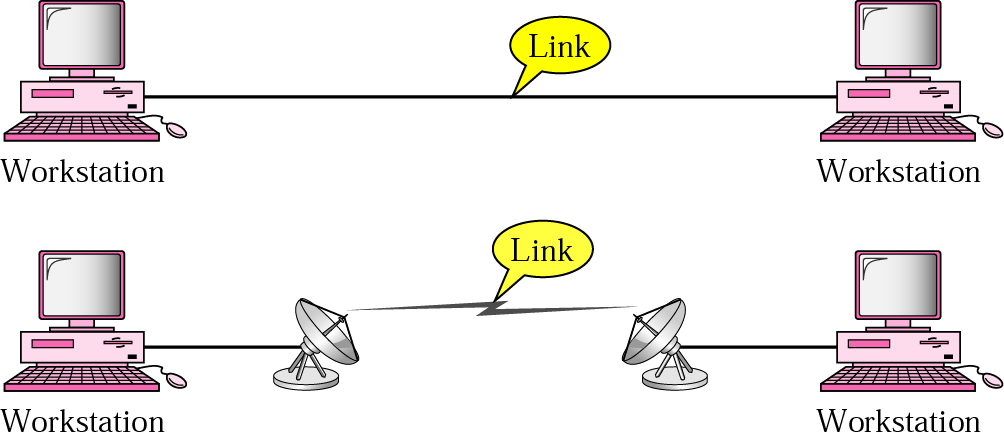
In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously.The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving.

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.

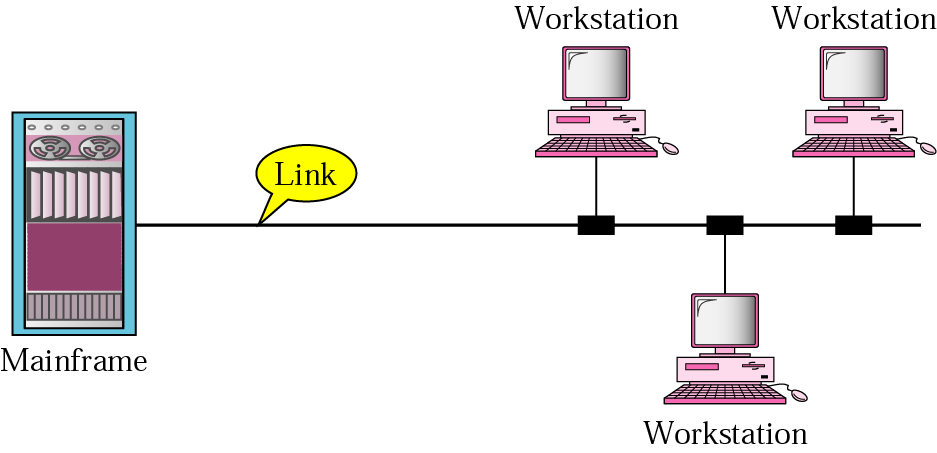
**Q. Explain types of connection.**

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections: point-to-point and multipoint.

**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. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible (see Figure 1.3a). When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.



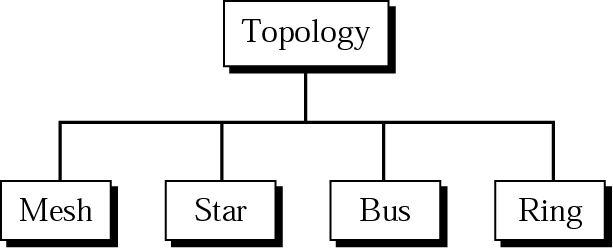
**Multipoint** A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure 1.3b). In a multipoint environment, the capacity ofthe channel is shared, either spatially or temporally. Ifseveral devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.



**Q. Explain criteria for selecting a topology.**

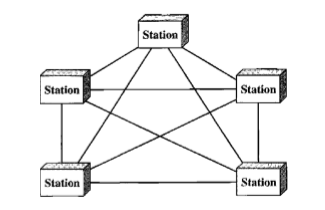
1. Size of Network
2. Number of nodes
3. Ease of Installation and Configuration
4. Security
5. Performance
6. Throughput
7. Scalability
8. Availability
9. Maintainability
10. Administrative ability
11. Cost
12. Future Growth
13. Cable Type
14. Connector type

**Q. Explain different Topologies in Networking.**

The term physical topology refers to the way in which a network is laid out physically.

**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. In a mesh topology, we need: n(n -1) /2

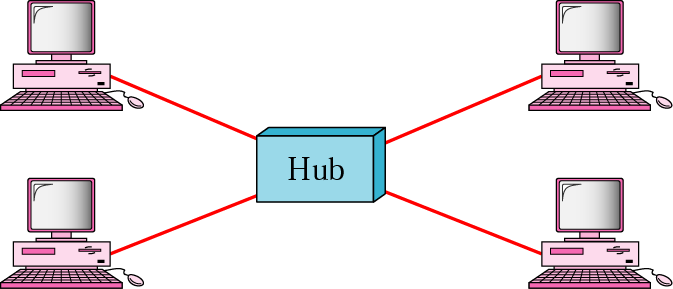


Duplex-mode links. To accommodate that many links, every device on the network must have n - 1 input/output (VO) ports (see Figure 1.5) to be connected to the other n - 1 stations.

A mesh offers several advantages over other network topologies. First, the use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices. Second, a mesh topology is robust. Ifone link becomes unusable, it does not incapacitate the entire system. Third, there is the advantage ofprivacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages. Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location ofthe fault and aids in finding its cause and solution.

The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required. First, because every device must be connected to every other device, installation and reconnection are difficult. Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate. Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive. For these reasons a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers ofa hybrid network that can include several other topologies.

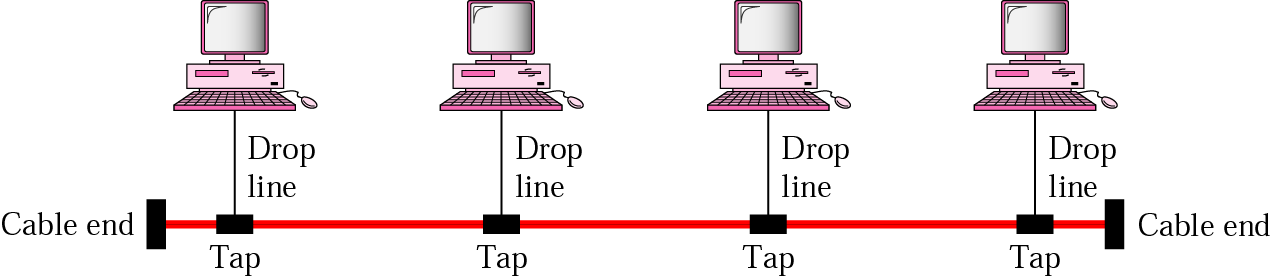
**Star Topology:**



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.

A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub. Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links. One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead. Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies.

**Bus Topology:**

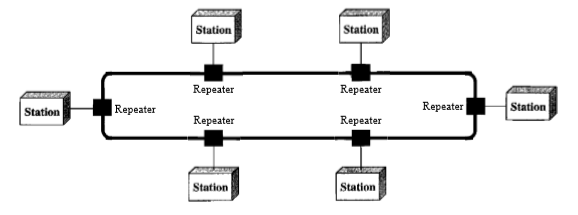
****

The preceding examples all describe point-to-point connections. A bus topology, on the otherhand, is multipoint. One long cable acts as a backbone to link all the devices in a network.

Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing ofa cable to create a contact with the metallic core. As a signal travels along the backbone, some ofits 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 oftaps a bus can support and on the distance between those taps. Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies.

Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone. In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side ofthe problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

**Ring Topology:**



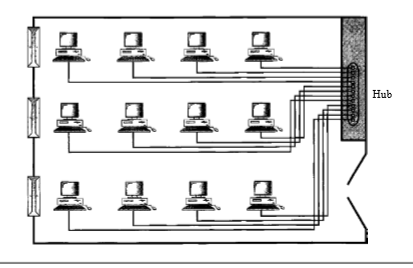
In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives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

A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location. However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

**Q. Explain Various Network Models.**

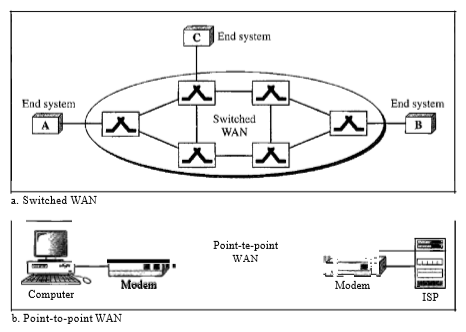
**Local Area Network (LAN)**

A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus (see Figure 1.10). Depending on the needs ofan organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometers. LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data. A common example of a LAN, found in many business environments, links a workgroup of task-related computers, for example, engineering workstations or accounting PCs. One of the computers may be given a large capacity disk drive and may become a server to clients. Software can be stored on this central server and used as needed by the whole group. In this example, the size of the LAN may be determined by licensing restrictions on the number ofusers per copy ofsoftware, orby restrictions on the number of users licensed to access the operating system. In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star. Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps.



**Wide Area Network (WAN)**

A wide area network (WAN) provides long-distance transmission ofdata, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. In Chapters 17 and 18 we discuss wide-area networks in greater detail. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet. We normally refer to the first as a switched WAN and to the second as a point-to-point WAN (Figure 1.11). The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN. The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (ISP). This type ofWAN is often used to provide Internet access.

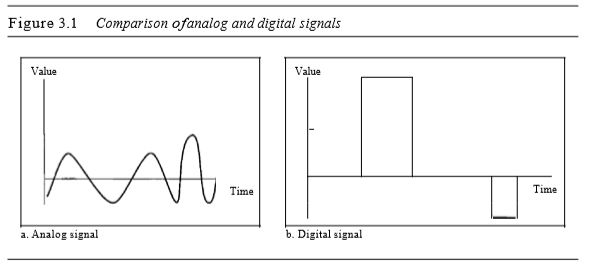


**Metropolitan Area Networks (MAN)**

A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part ofcity. A good example ofa MAN is the part ofthe telephone company network that can provide a high-speed DSL line to the customer. Another example is the cable TV network that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet. We discuss DSL lines and cable TV networks.

**Q. Define Analog and Digital signals.**

Data can be analog or digital. The term analog data refers to information that is continuous; digital data refers to information that has discrete states.Digital data take on discrete values.

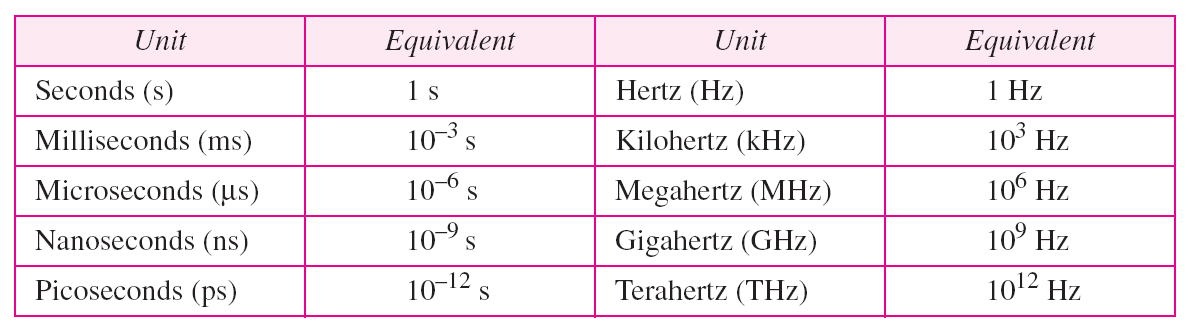


**Q. Define Periodic and Non-Periodic Signals.**

A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle. A non-periodic signal changes without exhibiting a pattern or cycle that repeats over time. Both analog and digital signals can be periodic or non-periodic.

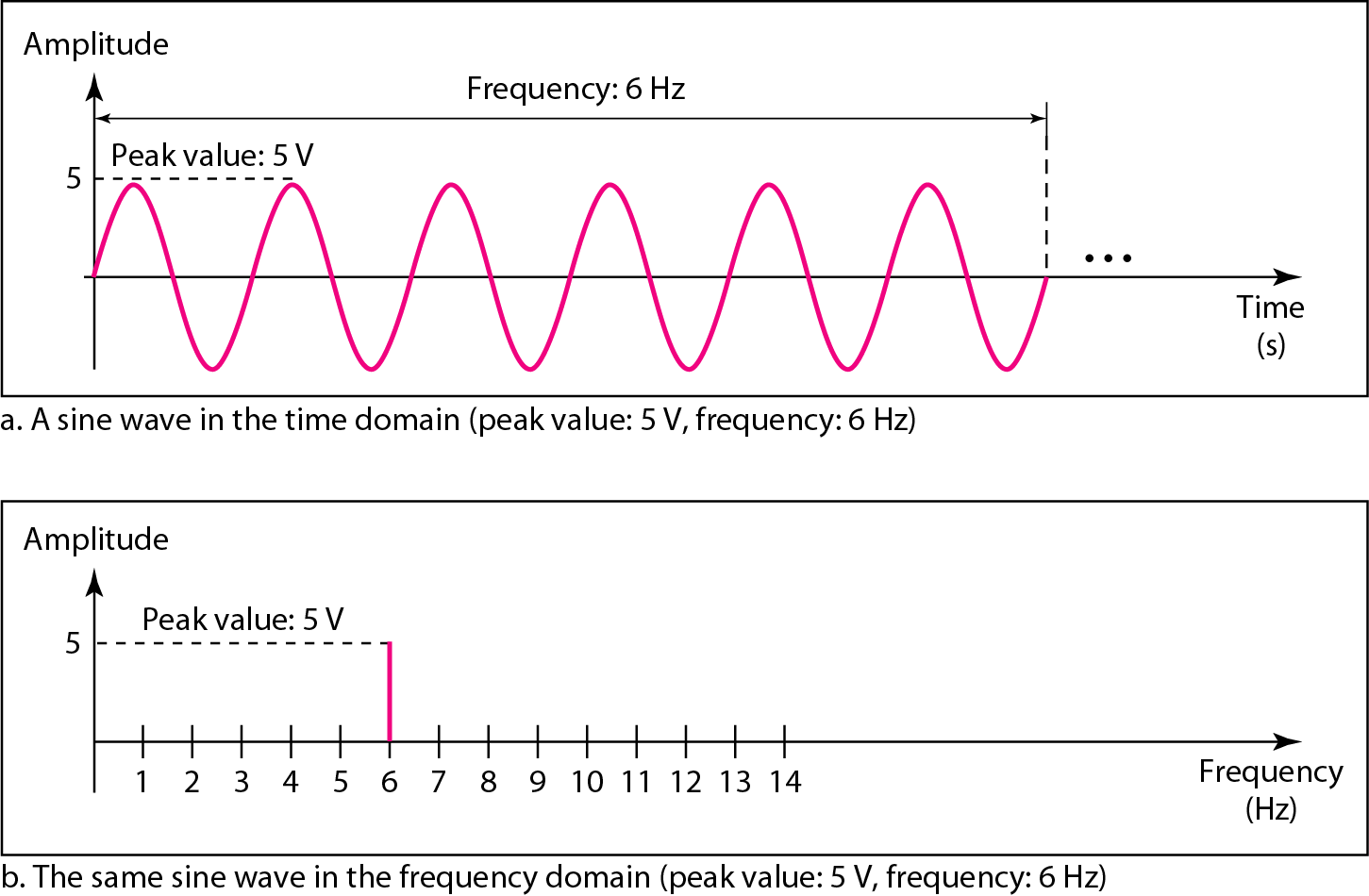
**Q. Explain Period and Frequency. Define High frequency & Low frequency**

Period refers to the amount of time, in seconds, a signal needs to complete 1 cycle. Frequency refers to the number ofperiods in I s. Frequency is the rate of change with respect to time.   
Change in a short span of time means high frequency. Change over a long span of time means low frequency.Note that period and frequency are just one characteristic defined in two ways. Period is the inverse offrequency, and frequency is the inverse ofperiod, as the following formulas show

****

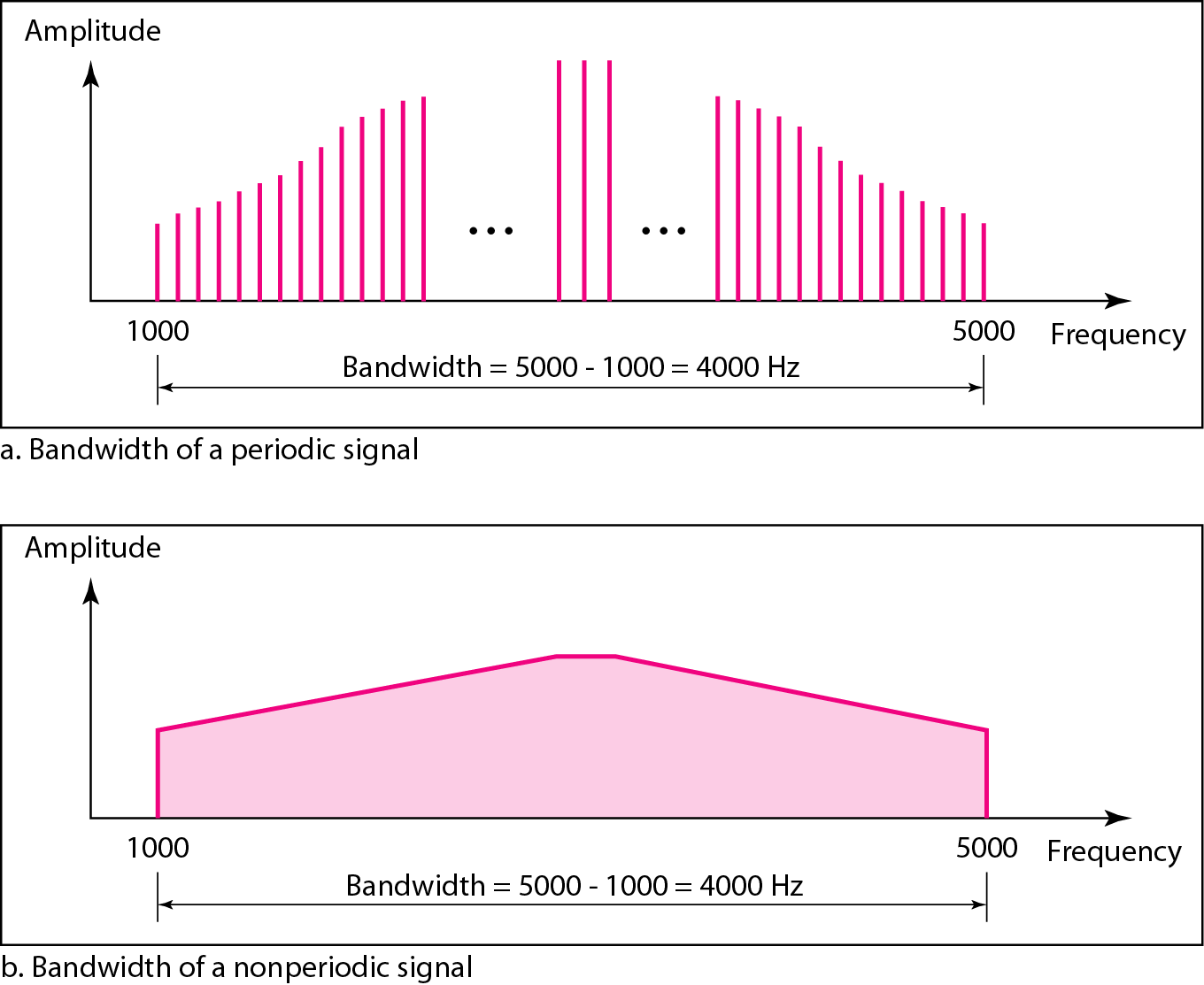
**Q. Explain Time and Frequency Domains**

A sine wave is comprehensively defined by its amplitude, frequency, and phase. We have been showing a sine wave by using what is called a time-domain plot. The time-domain plot shows changes in signal amplitude with respect to time (it is an amplitude-versus-time plot). Phase is not explicitly shown on a time-domain plot. To show the relationship between amplitude and frequency, we can use what is called a frequency-domain plot. A frequency-domain plot is concerned with only the peak value and the frequency.



**Q. Define Bandwidth**

The range of frequencies contained in a composite signal is its bandwidth. The bandwidth is normally a difference between two numbers. The bandwidth of a composite signal is the difference between the highest and the lowest frequencies contained in that signal.



**Q. Define Bit rate / Baud Rate/ Pulse rate**

The **data rate** (**Bit Rate**) defines the number of data elements (bits) sent in one second. The unit is bits per second (bps). The **baud** (**Symbol**) **rate** is the number of signal elements (symbols) sent in one second. The unit is the **baud**. The baud rate is sometimes called the **pulse rate**, the **modulation rate**, or the **signal rate**. The bit rate is the symbol rate multiplied by the number of bits per symbol.

**Q. Define Latency (Delay)**

The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source. We can say that latency is made of four components: propagation time, transmission time, queuing time and processing delay.

Latency = propagation time + transmission time + queuing time + processing delay

**Q. Explain Transmission Impairment**

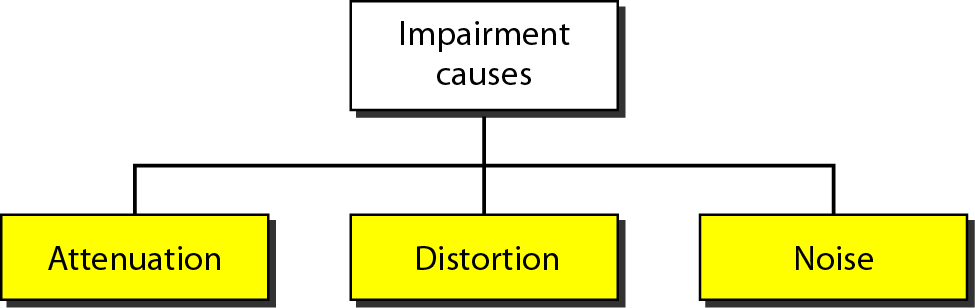
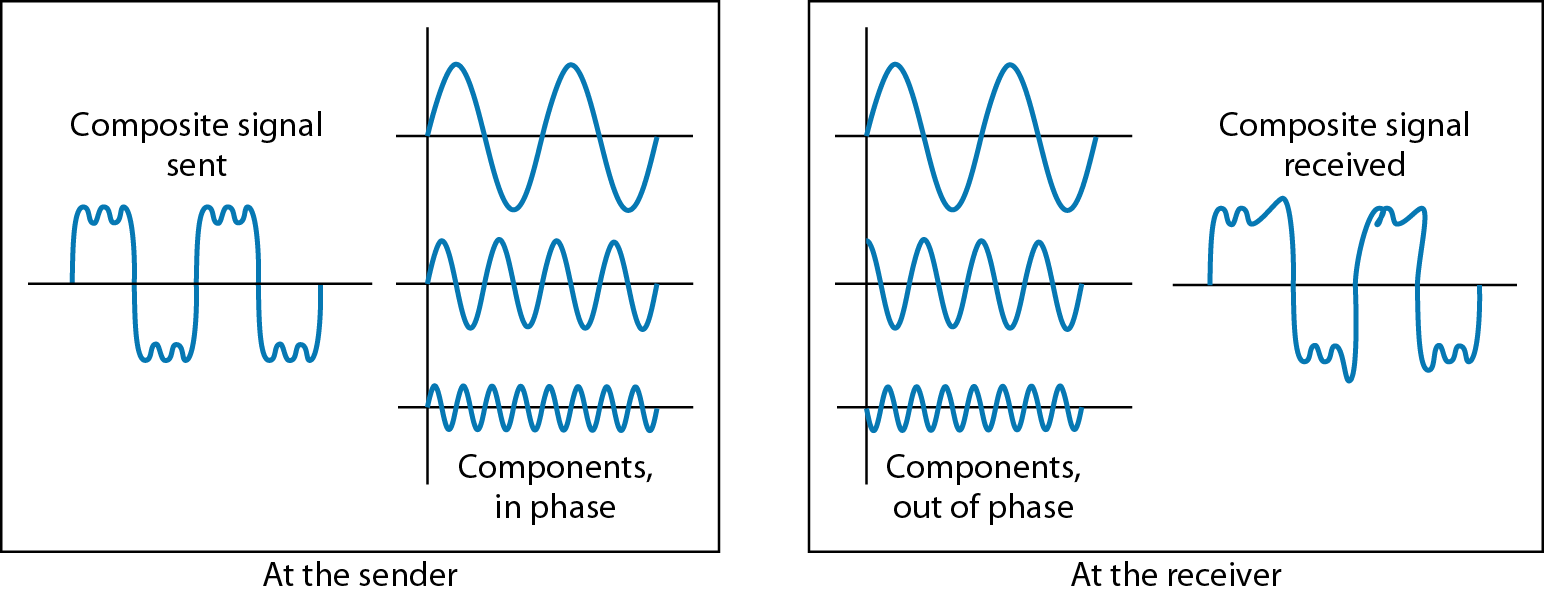
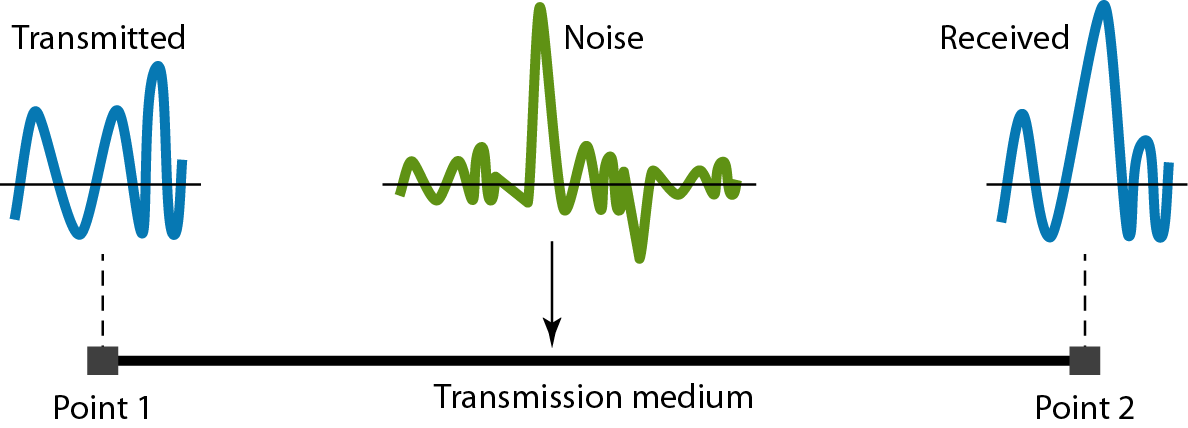


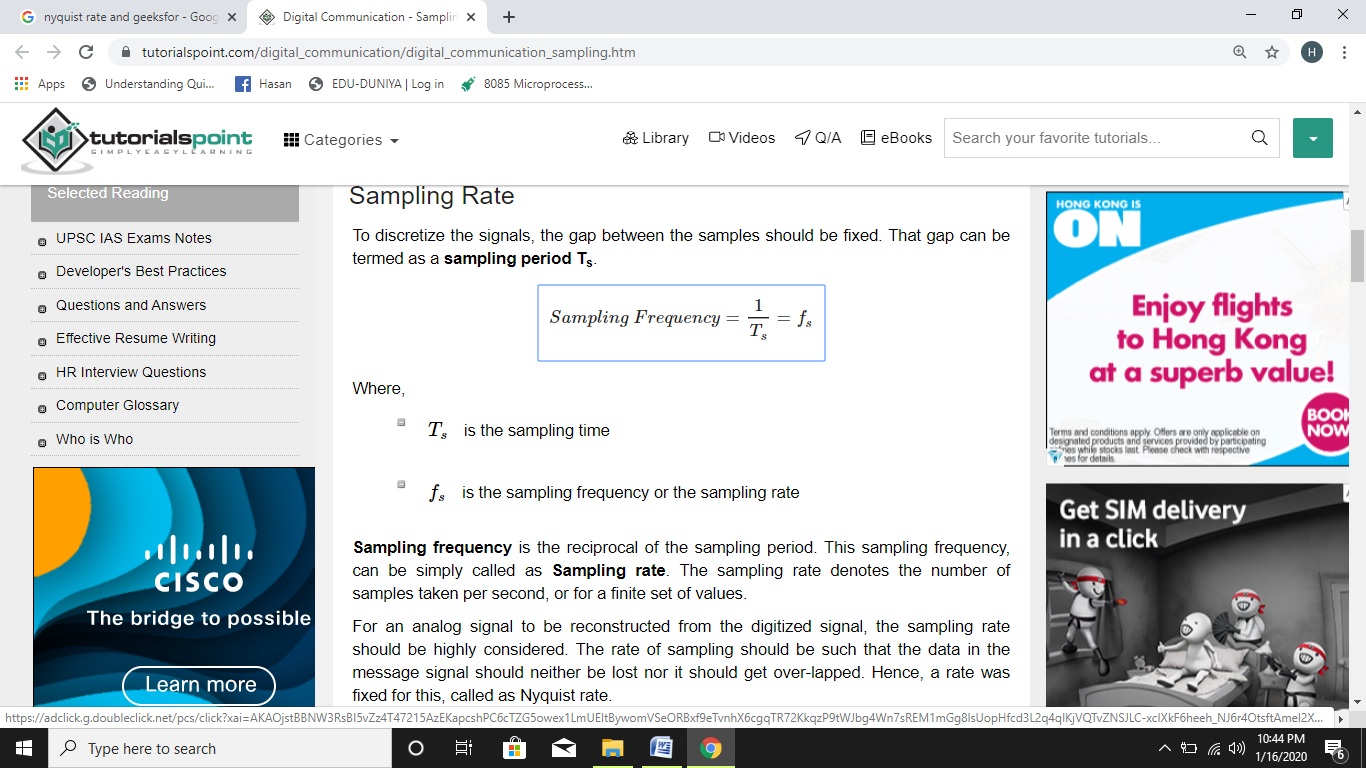
Fig: Attenuation effect

Fig: Effect of noise

**Q. Explain Nyquist Rate & Nyquist Formula. Define Shannon’s capacity**

**Sampling** is defined as, “The process of measuring the instantaneous values of continuous-time signal in a discrete form.”

Sampling Rate

To discretize the signals, the gap between the samples should be fixed. That gap can be termed as a **sampling period Ts**.

Where,

* Ts is the sampling time
* fs is the sampling frequency or the sampling rate

**Sampling frequency** is the reciprocal of the sampling period. This sampling frequency can be simply called as **sampling rate**. The sampling rate denotes the number of samples taken per second, or for a finite set of values.

For an analog signal to be reconstructed from the digitized signal, the sampling rate should be highly considered. The rate of sampling should be such that the data in the message signal should neither be lost nor it should get over-lapped. Hence, a rate was fixed for this, called as Nyquist rate.

**Nyquist Rate**

Suppose that a signal is band-limited with no frequency components higher than **W** Hertz. That means, **W** is the highest frequency. For such a signal, for effective reproduction of the original signal, the sampling rate should be twice the highest frequency.

fS=2W

Where,

* fS is the sampling rate
* **W** is the highest frequency

This rate of sampling is called as **Nyquist rate**.

**Sampling Theorem**

The sampling theorem, which is also called as **Nyquist theorem**, delivers the theory of sufficient sample rate in terms of bandwidth for the class of functions that are band limited.

The sampling theorem states that, “a signal can be exactly reproduced if it is sampled at the rate **fs** which is greater than twice the maximum frequency **W**.”

The Shannon capacity gives us the upper limit; the Nyquist formula tells us how many signal levels we need.

**THE OSI MODEL**

The OSI model facilitates communication between different systems without requiring changes to the logic of the underlying hardware and software. It is a model for understanding and designing a network architecture that is flexible, robust, and interoperable. It 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 (Figure 1)

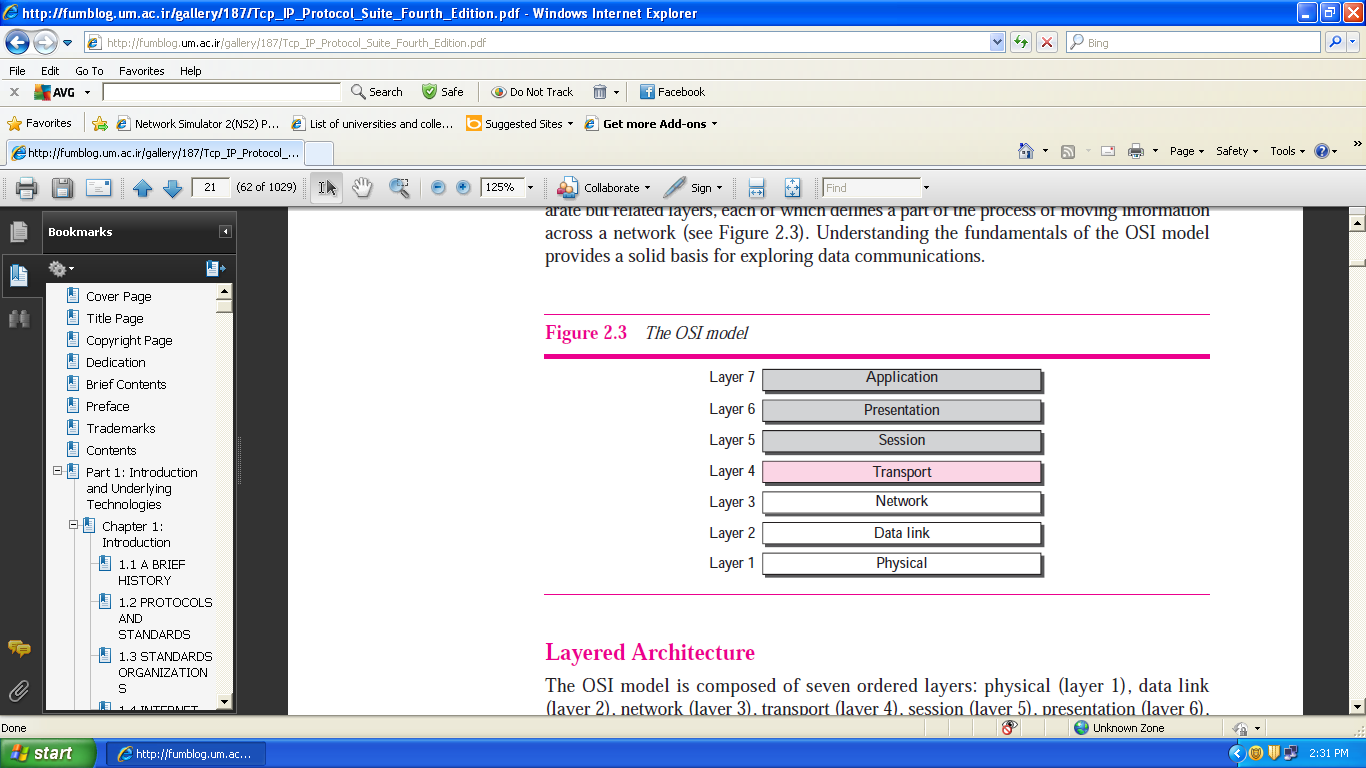


Fig 1 *The OSI model*

**Functions of Layers in the OSI Model:**

**Application Layer:** It allows access to network resources.

* **Network virtual terminal:** A software version of a physical terminal that allows a user to log on to a remote host.
* **File transfer, access, and management (FTAM):** 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 fore-mail forwarding and storage.
* **Directory Services:** This application provides distributed database sources and access for global information about various objects and services.

**Presentation Layer:** It translates, encrypts, and compresses data.

* Translation: 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**: 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.

**Session Layer**: It establishes, manages, and terminates sessions.

* **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 or full- mode.
* **Synchronization:** The session layer allows a process to add checkpoints (synchronization points) into a stream of data which ensures that the contents before check points are received and acknowledged. If any crash happens during the transmission, the only contents that need to be resent after system recovery are contents after synchronization checkpoints.

**Transport Layer:** It provides reliable process-to-process message delivery and error recovery.

* **Service-point addressing (or port addressing):** It addresses individual programs (or processes or tasks) on the host.
* **Segmentation and reassembly**: TL segments message in to segments at the source host and reassembles the segments in to message at the destination host.
* **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:** TL is responsible for end to end flow control (rather than across a single link as in the case of DLL).
* **Error control**: TL is responsible for process-to-process error control (rather than across a single link as in the case of DLL). 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.

**Network Layer:** It moves packets from source to destination and provides internetworking.

* **Logical addressing**: The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical (IP) addresses of the sender and receiver.
* **Routing**: When independent networks or links are connected together to create internetworks 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.

**Data link Layer:** It organizes bits into frames and provides hop-to-hop (node-to-node) delivery.

* **Framing**: The data link layer divides the stream of bits received from the network layer into manageable data units called frames*.*
* **Physical addressing**: The physical address, also known as the link address, is the address of a node as defined by its LAN (host address) or WAN (Router address). It is included in the frame used by the data link layer. It is the lowest-level address. For example, Ethernet uses a 6-byte physical address that is imprinted on the network interface card (NIC) of host or router.
* **Flow control**: If the rate at which the data is absorbed by the receiver is less than the rate produced at the sender, the data link layer imposes a flow control mechanism to prevent 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.

**Physical Layer**: It transmits bits over a medium and provides mechanical and electrical specifications.

* **Physical characteristics of interfaces and media:** The physical layer defines the characteristics of the interface between the devices and the transmission media. It also defines the type of transmission media.
* **Representation of bits**: The physical layer defines the type of encoding (how 0s and 1s are changed to signals).
* **Data rate**: The transmission rate—the number of bits sent each second—is defined by the physical layer.
* **Synchronization of bits:** The sender and receiver 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 together through a dedicated link. In a multipoint configuration, a link is shared between several devices.
* **Physical topology:** The physical topology defines how devices are connected to make a network. Devices can be connected using a mesh, a star, a ring, or a bus topology.
* **Transmission mode:** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

**Q1. Explain TCP/IP protocol suit.**

**TCP/IP Protocol Suit**

The TCP/IP protocol suit is made up of four layers: host-to-network, internetwork, transport, and application as shown in figure2.

.

**Application Layer**

SMTP

FTP

TFTP

HTTP

DNS

SNMP

TELNET

DHCP

• • •

**Transport Layer**

SCTP

TCP

UDP

**Internetwork Layer**

IP

ICMP

IGMP

ARP

RARP

**Host-To-Network Layer**

**Figure 2** *TCP/IP protocol suit*

Different layers and protocols used in them are explained below:

**Host-to-Network Layer Protocols**

At this layer TCP/IP does not define any specific protocol. It supports all of the standard and proprietary protocols.

**Internetwork Layer Protocols**

The internetwork (internet in short) layer is responsible for host to host (source host to destination host) delivery of datagrams possibly across multiple networks. Internet layer supports **Internet Protocol (IP).** IP uses four supporting protocols: **ARP, RARP, ICMP, AND IGMP.**

**IP:** It is an unreliable and connectionless datagram protocol – a *best effort delivery* service. The best effort means that IP provides no error checking or tracking, i.e., it does its best to get a transmission through to its destination, but with no guarantees. IP transports data in packets called datagrams.

**Address Resolution Protocol (ARP):** ARP is a dynamic method to map an IP address to its physical address. Any time a host or a router needs to find the physical address of another host or router on its network, it broadcasts an ARP query packet which includes the physical and IP addresses of the sender and IP address of the receiver. The intended recipient recognizes its IP address and sends back an ARP response packet which contains the recipient’s IP and physical addresses.

**Reverse Address Resolution Protocol (RARP):** RARP allows a host to discover its IP address when it knows only its physical address. It is used when a computer is connected to the network for the first time or when a diskless computer is booted.

**Internet Control Message Protocol (ICMP):** ICMP is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. ICMP sends query messages (echo request or reply, time-stamp request or reply, address mask request or reply, and router solicitation or advertisement) and error reporting messages (destination unreachable, source quench, time exceeded, parameter problem, and redirection).

**Internet Group Management Protocol (IGMP):** IGMP is a companion protocol of IP that is used to facilitate the simultaneous transmission of a message to a group of recipients (called IP multicasting) . It is not a routing protocol but a protocol that manages the group membership. For example, multiple stock brokers can simultaneously be informed of changes in a stock price, or travel agents can be informed of a trip cancellation. Some other applications include distance learning or video on demand.

**Transport Layer Protocols**

Transport layer is responsible for the delivery of a message or byte stream from one process to another. Transport layer contains three protocols: **User Datagram Protocol (UDP), Transmission control Protocol (TCP), and Stream Control Transmission Protocol (SCTP).**

**UDP:**

* A process-to-process, connectionless, unreliable, and message-oriented transport protocol.
* Provides no flow control, , no error control, and no congestion control.
* Performs very limited error checking by adding a checksum field in the header of user datagram. Corrupt user datagrams are discarded.
* A very simple protocol that requires little overhead (fixed-size header of 8 bytes) and offers fast delivery.
* Uses multiplexing and demultiplexing to handle several processes simultaneously.
* UDP packet is called user datagram.
* Applications: FTP, TFTP, multicasting, SNMP, route update protocols and real-time applications.

**TCP:**

* A process to process, full duplex, connection-oriented, reliable, and byte-oriented transport protocol.
* Provides flow control, error control, and congestion control.
* A complex and slower protocol with variable – size header ranging from 20 bytes to 60 bytes.
* A TCP packet is called a segment.
* Uses multiplexing and demultiplexing to handle several processes simultaneously.
* Application: data transfer.

**SCTP:**

* A process to process, full duplex, connection-oriented, reliable, and message-oriented transport protocol that combines the best features of UDP and TCP. An SCTP connection is called **association**.
* SCTP provides additional services not provided by UDP or TCP, such as **multiplestream** and **multihoming** services. These two services provide fast delivery of packets.
* Provides flow control, error control, and congestion control.
* The general header in SCTP is only 12 bytes.
* SCTP uses a term packet to define a transportation unit.
* SCTP is mostly designed for Internet applications that have recently been introduced (sophisticated multimedia applications). These new applications such as IUA (ISDN over IP), M2UA and M3UA (telephony signaling), H.248 (media gateway control), H.323 (IP telephony), and SIP (IP telephony), need more sophisticated service than TCP can provide. SCTP provides this enhanced performance and reliability.

**Application Layer Protocols**

Application layer allows a user to access the services of a network such as electronic mail, file access and transfer, access to system resources, surfing the World Wide Web, and network management.

* **Simple Mail Transfer Protocol (SMTP):** This protocol defines Message Transfer Agent (MTA) client and server in mail server to transfer mail from the sender to receiver’s mailbox.
* **File Transfer Protocol (FTP):** FTP is a TCP/IP client server application for copying a file from one host to another.
* **Trivial File Transfer Protocol (TFTP):** TFTP is a simple client server protocol without the complexities and sophistication of FTP. For example, when a diskless workstation or a router is booted, we need to download bootstrap and configuration files. TFTP is designed for these types of file transfers.
* **Domain Name System (DNS):** DNS is a client server application program used to map a host name in the application layer to an IP address in the network layer.
* **Simple Network Management Protocol (SNMP):** SNMP is a framework for managing devices in an Internet using the TCP/IP protocol suit.
* **Terminal Network (TELNET):** TELNET is a virtual terminal protocol that enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system.
* **Dynamic Host Configuration Protocol (DHCP):** DHCP is a static as well as dynamic configuration protocol that provides the following four information to either diskless computers or computers at first boot:

1. The IP address of the computer,
2. The subnet mask of the computer,
3. The IP address of a router, and
4. The IP address of a name server.

**Difference between a protocol, a Service and an interface**

Each layer performs some ***services*** for the layer above it. The **service** definition tells what the layer does, not how entities above it access it or how the layer works. It defines the layer’s semantics.

A layer’s ***interface*** tells the processes above it how to access it. It specifies what the parameters are and what results to expect. It, too, says nothing about how the layer works inside.

Finally, the peer ***protocols*** used in a layer are the layer’s own business. It can use any protocols it wants to, as long as it gets the job done (i.e., provides the offered services). It can also change them at will without affecting software in higher layers.

**Q. Differentiate between connection-oriented and connectionless services.**

|  |  |
| --- | --- |
| **Connection – Oriented Service** | **Connectionless Service** |
| A connection is first established (through signaling), which is usually accompanied by some form of resource reservation. After data transfer is over, the connection is released. | A connection does not need to be established before data exchanged. Thus, there is hardly any prior resource reservation. |
| The services are generally reliable in the sense that the data loss is either minimal or there are mechanisms to retransmit the lost data. | The scheme provides unreliable or best-effort services in the sense that lost or dropped packets are not retransmitted. |
| The transfer mode for a connection-oriented is circuit-switching or virtual circuit-switching. | The transfer mode for a connectionless service is routing. |
| For a packet-based connection-oriented service, the packets are delivered sequentially (i.e. the packets for a connection follow the same path). | Packets may or may not arrive sequentially (i.e. data packets may or may not follow the same path). |
| Further, packets do not carry the full address of the destination. Due to this, the header size is small and per packet overhead of the scheme is minimal. | Packets carry the full address of the destination to enable routing. Due to this, the header size is large and the per packet overhead of the scheme can be significant. |
| The scheme is suitable for long and steady transmission. | The scheme is suitable for bursty transmissions. |