UNIT-1

NETWORKS

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

Network Criteria

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

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.

Performance is often evaluated by two networking metrics: throughput and delay.

Reliability

In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure.

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.

NETWORK GOALS:

- The main goal of networking is "**Resource sharing**", and it is to make all programs, data and equipment available to anyone on the network without the regard to the physical location of the resource and the user.
- A second goal is to provide **high reliability** by having alternative sources of supply. For example, all files could be replicated on two or three machines, so if one of them is unavailable, the other copies could be available.
- Another goal is **saving money**. Small computers have a much better price/performance ratio than larger ones. Mainframes are roughly a factor of ten times faster than the fastest single chip microprocessors, but they cost thousand times more.
- Another closely related goal is to increase the systems performance as the work load increases by just adding more processors.

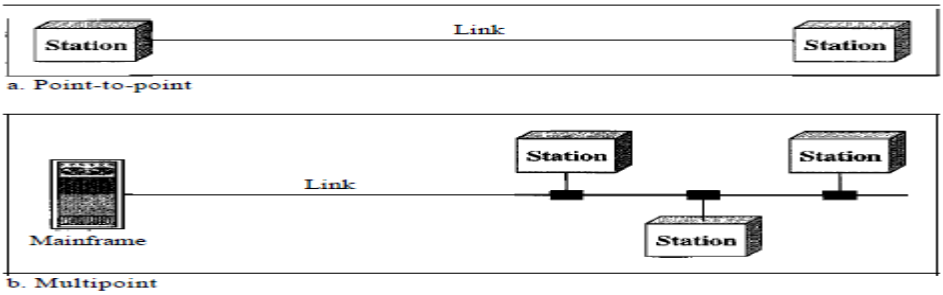
NETWORK APPLICATIONS:

- Access to remote programs.
- Access to remote databases.
- E-commerce
- Person to person communication.

Type of Connection

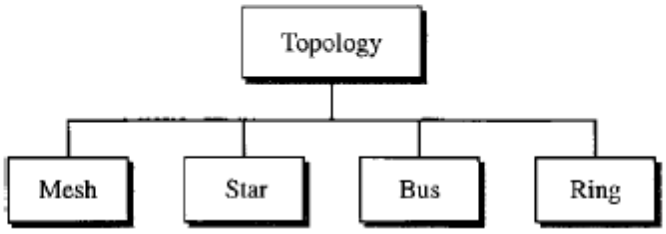
There are two possible types of connections: point-to-point and multipoint.

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.
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.

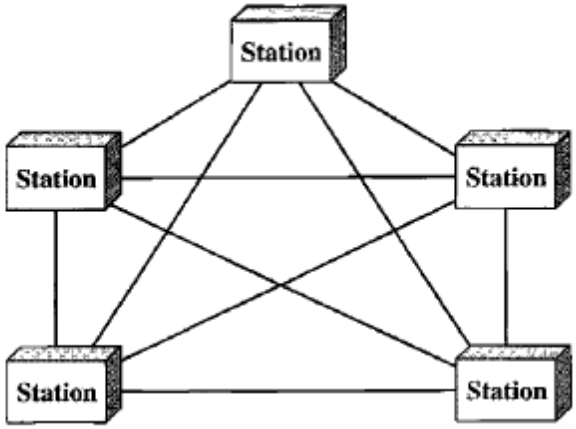


Physical Topology
The term physical topology refers to the way in which a network is laid out physically.

Categories of topology



Mesh 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. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to n - I nodes, node 2 must be connected to n - 1 nodes, and finally node n must be connected to n - 1 nodes. We need n(n - 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need n(n -1) /2 duplex-mode links.

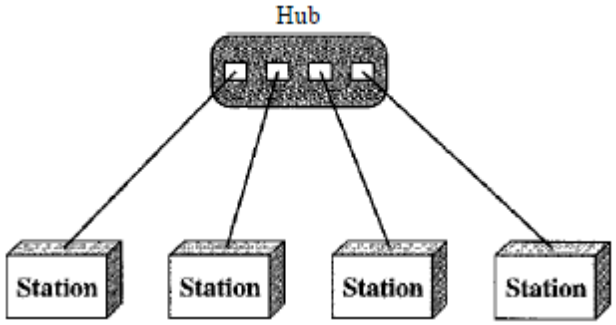


Advantage:
A mesh offers several advantages over other network topologies. First, the use ofdedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
Second, a mesh topology is robust. If one link becomes unusable, it does not incapacitate
the entire system.
Third, there is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it.
Finally, point-to-point links make fault identification and fault isolation easy

Disadvantage:

The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required. Installation and reconnection are difficult.
Hardware required to connect each link (I/O ports and cable) can be expensive

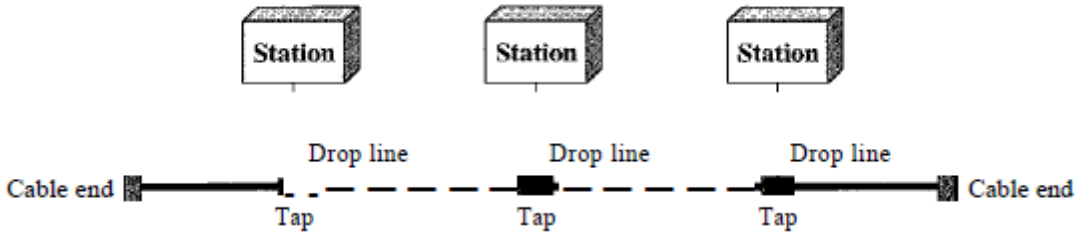
Star Topology
In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: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



Advantage:
Less Expensive than a mesh topology
Robust

Disadvantage:
Single point failure i.e central controller Hub.

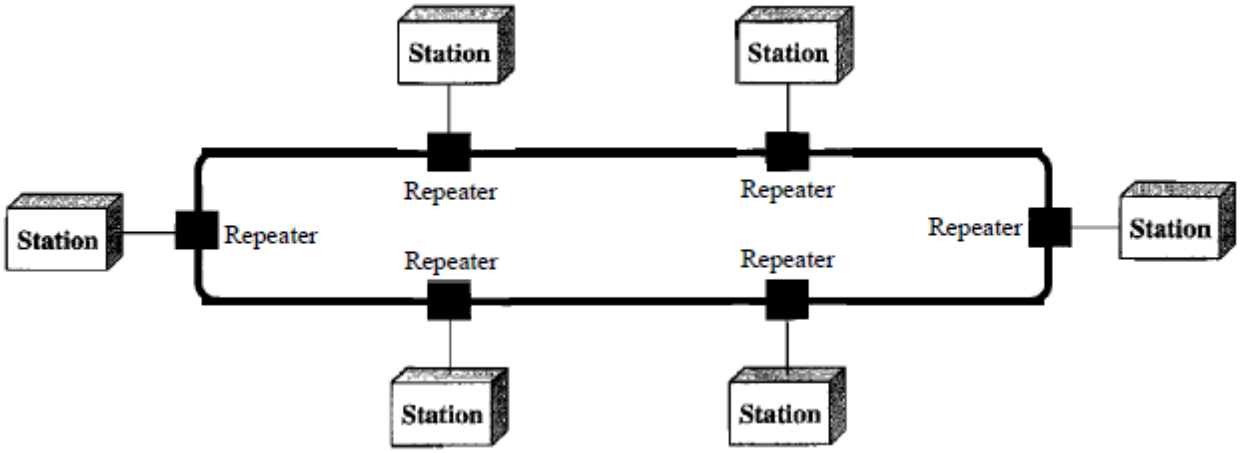
Bus topology:
A **bus topology has** multipoint connection. One long cable acts as a **backbone** to link all the devices in a networkNodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector.



Advantage:
Ease of installation
Less cable required

Disadvantage:
Heavy traffic slows down the speed.
Difficult reconnection and fault isolation.
Fault in backbone cable stops all transmission.

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



Advantage:
Easy to install and configure.
Fault isolation easy.

Disadvantage:
Unidirectional traffic which can be eliminated by dual ring.

OSI Model
An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model. It was first introduced in the late 1970s. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is

to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable. 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 layers.

Physical Layer

The physical layer is responsible for movements of individual bits from one hop (node) to the next.

The physical layer is also concerned with the following:
Physical characteristics of interfaces and medium The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
Representation of bits: 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 andthe 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.
Transmission mode The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

Data Link Layer
The data link layer is responsible for moving frames from one hop (node) to the next.
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 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.

Network Layer

The network layer is responsible for the delivery of individual packets from the source host to the destination host.

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 the delivery of a message from one process to another.

Responsibilities of the network layer include the following:

Service-point addressing- The transport layer header includes a type of address called a service-point address (or port address) so that process can communicate with each other.

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- The transport layer is responsible for flow control which is end to end.

Error control- The transport layer is responsible for error control.

Session Layer

The session layer is responsible for dialog control and synchronization.

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 responsible for translation, compression, and encryption.

Translation-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 is responsible for providing services to the user. It is responsible for providing services like network virtual terminal, mail services, file transfer services etc.

TCP/IP PROTOCOL SUITE

The TCPIIP protocol suite was developed prior to the OSI model. TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the host-to-network layer is equivalent to the combination of the physical and data link layers. The internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCPIIP taking care of part of the duties of the session layer.

Comparison of OSI Model and TCP/IP protocol suite

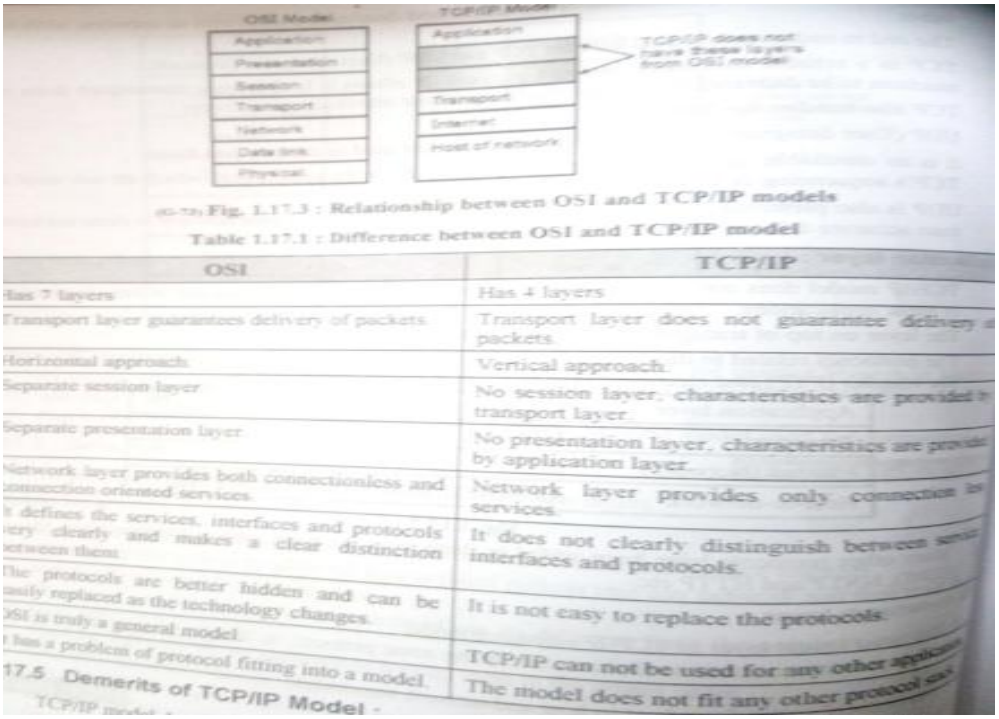


Fig. 1.17.3 : Relationship between OSI and TCP/IP models

Table 1.17.1 : Difference between OSI and TCP/IP model

OSI	TCP/IP
Has 7 layers	Has 4 layers
Transport layer guarantees delivery of packets.	Transport layer does not guarantee delivery of packets.
Horizontal approach.	Vertical approach.
Separate session layer.	No session layer, characteristics are provided by transport layer.
Separate presentation layer.	No presentation layer, characteristics are provided by application layer.
Network layer provides both connectionless and connection oriented services.	Network layer provides only connection less services.
It defines the services, interfaces and protocols very clearly and makes a clear distinction between them.	It does not clearly distinguish between services, interfaces and protocols.
The protocols are better hidden and can be easily replaced as the technology changes.	It is not easy to replace the protocols.
OSI is truly a general model.	TCP/IP can not be used for any other application.
It has a problem of protocol fitting into a model.	The model does not fit any other protocol suite.

17.5 Demerits of TCP/IP Model :

Delay

Processing Delay is the time that is taken by the router to access the header of a packet and redirect it to the next path.

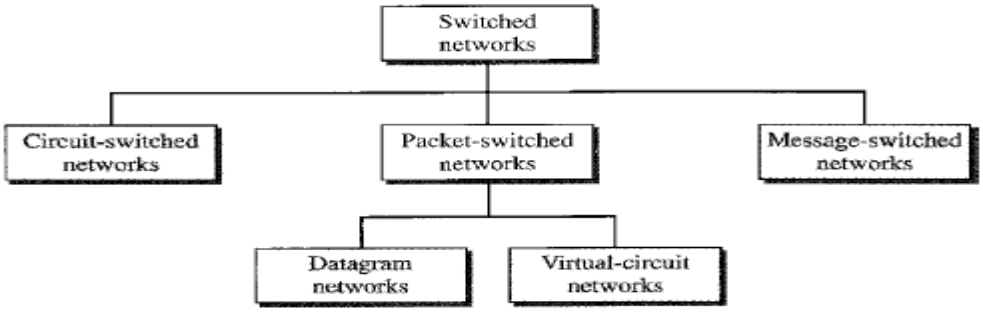
Queuing Delay is the time that a packet has to wait in the queue before it can be transmitted over the link. Packets are put in the queue when the speed of incoming link to the router is faster than the outgoing link. Queuing delay depends on the number of earlier arrived packets already waiting for getting transmitted. If the queue is empty, then the queuing delay is zero, and if the traffic or the number of incoming packets is high, then the queuing delay is high.

Transmission delay is usually caused by the data rate of the link. It is the time taken to push all the packet bits on to the link.

Propagation Delay is the time taken by the 1st bit of the packet to reach the receiver router. It can be calculated by dividing the distance between the two routers and the speed of propagation of the link.

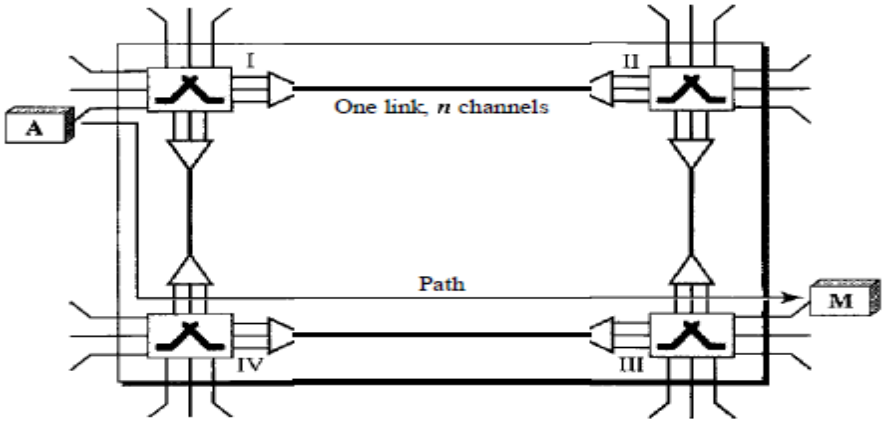
Switching Method

A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing. Three methods of switching have been important: circuit switching, packet switching, and message switching.



Circuit-switched network

A circuit-switched network is made of a set of switches connected by physical links, in which each link is divided into n channels. Circuit switching takes place at the physical layer.



The actual communication in a circuit-switched network requires three phases: connection setup, data transfer, and connection teardown.

Setup Phase

Before the two parties (or multiple parties in a conference call) can communicate, a dedicated circuit (combination of channels in links) needs to be established. The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches.

Data Transfer Phase

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

Teardown Phase

When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

Efficiency

Circuit-switched networks are not as efficient as the other two types of networks because resources are allocated during the entire duration of the connection. These resources are unavailable to other connections.

Delay

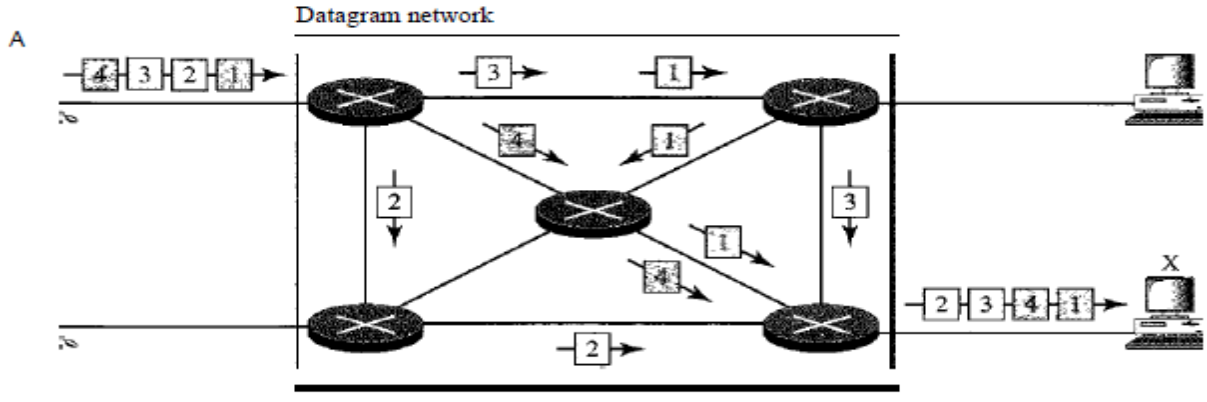
Although a circuit-switched network normally has low efficiency, the delay in this type of network is minimal. During data transfer the data are not delayed at each switch; the resources are allocated for the duration of the connection.

Packet Switching

In data communications, we need to send messages from one end system to another. If the message is going to pass through a packet-switched network, it needs to be divided into packets of fixed or variable size. The size of the packet is determined by the network and the governing protocol. In packet switching, there is no resource allocation for a packet and it is allocated on-demand.

Datagram Network

In a datagram network, each packet is treated independently of all others. Even if a packet is part of a multipacket transmission, the network treats it as though it existed alone. Packets in this approach are referred to as datagrams. Datagram switching is normally done at the network layer.



The datagram networks are sometimes referred to as connectionless networks. The term connectionless here means that the switch (packet switch) does not keep information about the connection state. There are no setup or teardown phases. Each packet is treated

the same by a switch regardless of its source or destination. In this type of network, each switch (or packet switch) has a routing table which is based on the destination address. The routing tables are dynamic and are updated periodically. The destination addresses and the corresponding forwarding output ports are recorded in the tables. Switching in the Internet is done by using the datagram approach to packet switching at the network layer.

Efficiency

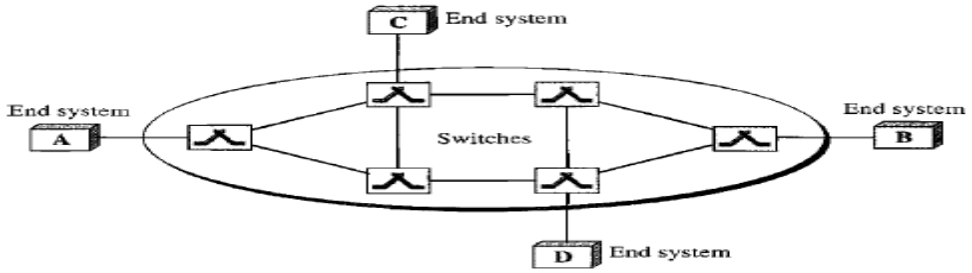
The efficiency of a datagram network is better than that of a circuit-switched network; resources are allocated only when there are packets to be transferred.

Delay

There may be greater delay in a datagram network than in a virtual-circuit network. Although there are no setup and teardown phases, each packet may experience a wait at a switch before it is forwarded.

VIRTUAL-CIRCUIT NETWORKS

A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.



Global Addressing

A source or a destination needs to have a global address-an address that can be unique in the scope of the network or internationally.

Virtual-Circuit Identifier

The identifier that is actually used for data transfer is called the virtual-circuit identifier (VCI). A VCI, unlike a global address, is a small number that has only switch scope. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCI.

Three Phases

As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: setup, data transfer, and teardown. In the setup phase, the source and destination use their global addresses to help switches make table entries for the connection. In the teardown phase, the source and destination inform the switches to delete the corresponding entry. Data transfer occurs between these two phases.

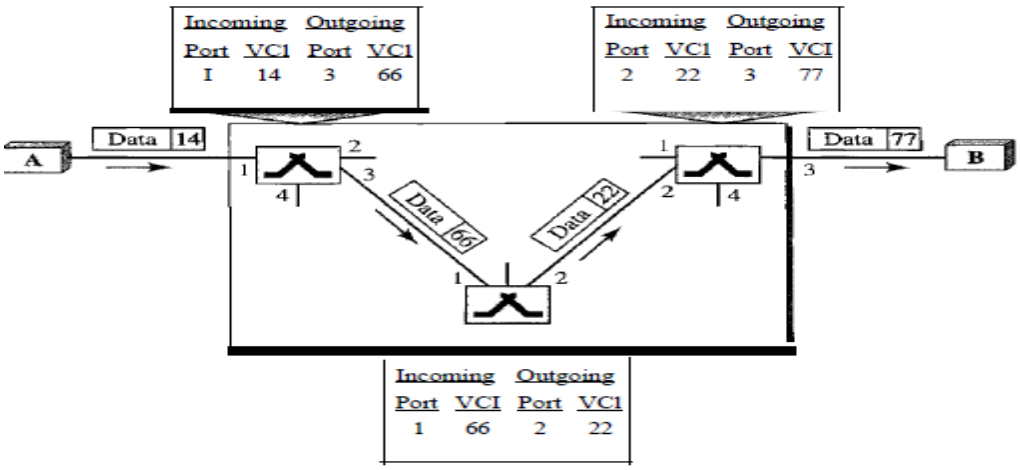


Fig. Source to destination data transfer in virtual circuit network

Efficiency

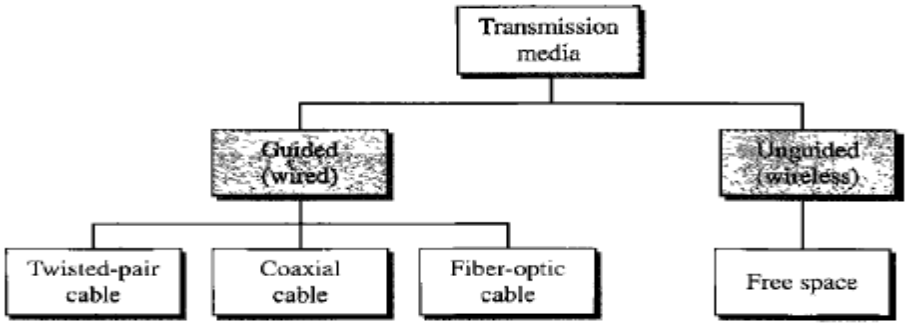
As we said before, resource reservation in a virtual-circuit network can be made during the setup or can be on demand during the data transfer phase. In the first case, the delay for each packet is the same; in the second case, each packet may encounter different delays.

Comparison of circuit switching, packet switching and message switching

Parameter	Message switching	Circuit switching	Packet switching
Application	Telegraph network for transmission of telegrams.	Telephone network for bi-directional, real time transfer of voice signals.	Internet for datagram and reliable stream service between computers.
End terminal	Telegraph, teletype.	Telephone, modem.	Computer
Information type	Data in the form of Morse, Baudot, ASCII codes.	Analog voice or PCM digital voice	Binary information
Transmission system	Digital data over different transmission media	Analog and digital data over different transmission media	Digital data over different transmission media.
Addressing scheme	Geographical addresses	Hierarchical numbering plan	Hierarchical address space
Routing scheme	Manual	Route selected during call setup.	Each packet is routed independently.
Multiplexing scheme	Character or message multiplexing	Circuit multiplexing.	Packet multiplexing shared media access networks.

Transmission Media

A transmission **medium** can be broadly defined as anything that can carry information from a source to a destination.



GUIDED MEDIA

Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.

Twisted-Pair Cable- A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown in Figure

One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals. If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources (e,g., one is closer and the other is farther). This results in a difference at the receiver. By twist,ing the pairs, a balance is maintained.

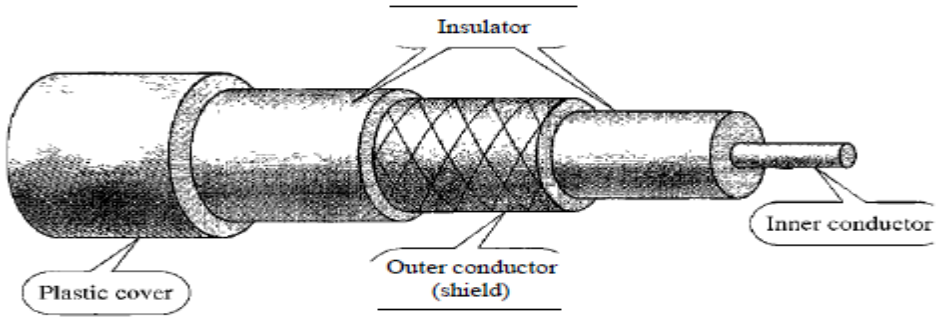
Unshielded Versus Shielded Twisted-Pair Cable

The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP). IBM has also produced a version of twisted-pair cable for its use called shielded twisted-pair (STP). STP cable has a metal foil covering that encases each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.

Coaxial Cable

Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently. 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. The outer metallic wrapping

serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover



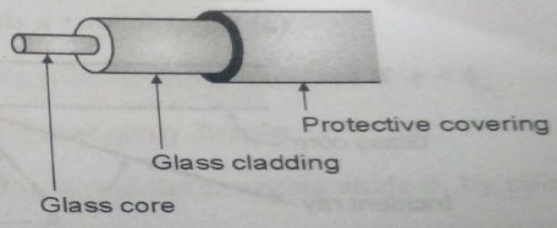
Fiber-Optic Cable

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.

The construction of an optical fiber cable is as shown in Fig. 2.7.1.

It consists of an inner glass core surrounded by a glass cladding which has a lower refractive index and a protective covering.

Digital signals are transmitted in the form of intensity - modulated light signal.



(G-103) **Fig. 2.7.1 : Construction of optical fiber cable**

Light is launched into the fiber at one end using a light source such as a light emitting diode (LED) or laser.

It is detected on the other side using a photo detector such as a phototransistor or photodiode.

Unguided (wireless) Media

An unguided media does not use a conductor or wire as a communication channel. It uses air or vacuum as medium to carry information from transmitter to receiver. The transmitter first converts the data signal into electromagnetic waves and transmits then using a suitable antenna. The receiver receives them using a receiving antenna and converts electromagnetic waves in to data signal.

Types of wireless media

Radio wave

Microwave

Infrared

ISDN(Integrated service digital network)

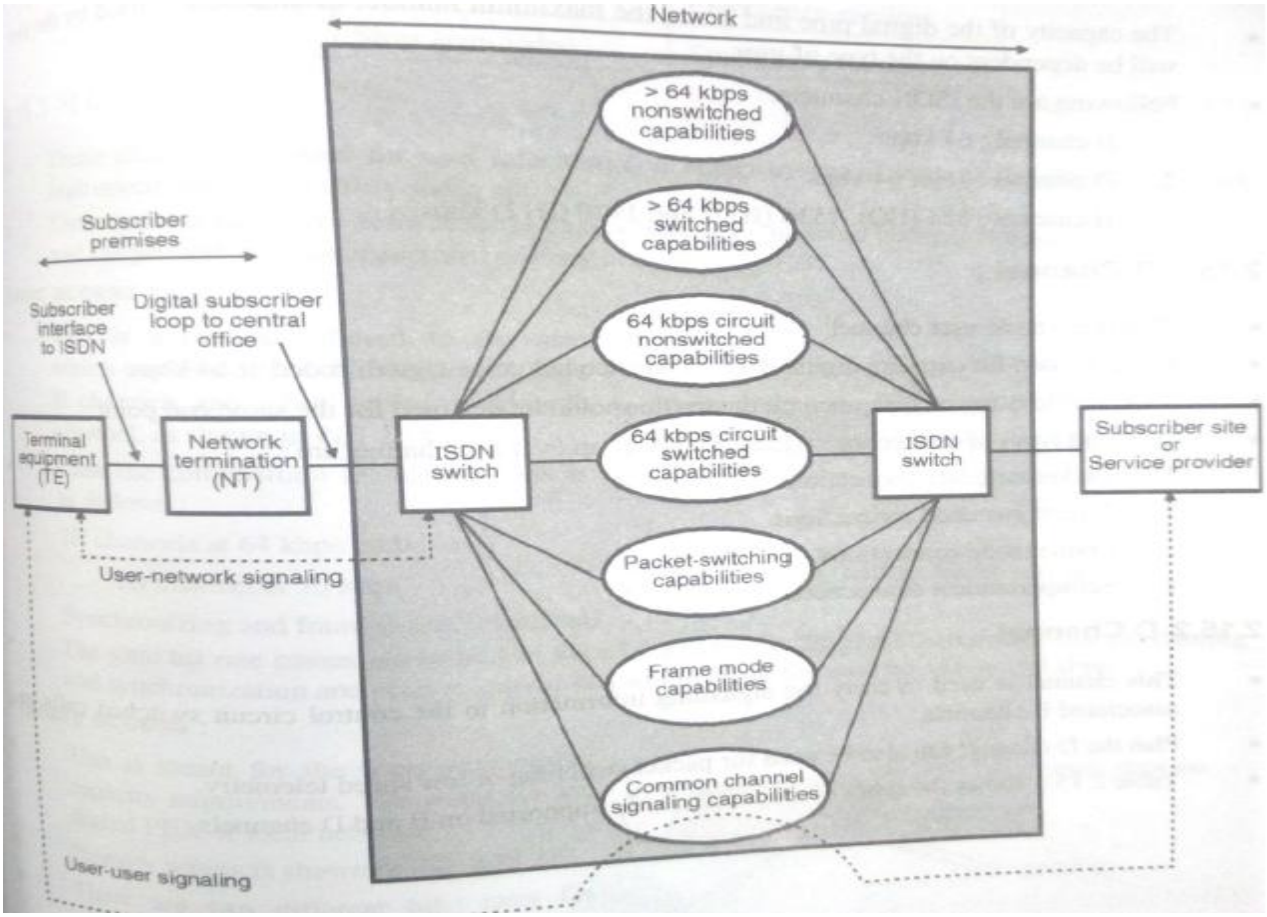
ISDN is a set of communication standard for simultaneous digital transmission of voice, video, data and other network services over the traditional circuit of public switched telephone network(PSTN).

There are two types of ISDN

(1) **Narrowband ISDN-** It has smaller bandwidth and it can support the data rate of 64kbps only. Due to low data rate the quality of service provide by it is poor. It uses copper wire for transmission.

(2) **Broadband ISDN**- It provides higher data rates and it can support the data rate of 128kbps. Due to high data rate the quality of service provide by it is good. It uses optical fiber for transmission.

Architecture of ISDN



(Architecture explained in class)

ISDN services

ISDN is capable of providing following services:

- Existing voice applications
- Data applications
- FAX
- Teletext services
- Videotext services

ISDN Channel

- B channel: 64 kbps
- D channel: 16 or 64 kbps

- H channel

Connecting devices

Passive Hubs
A passive hub is just a connector. It connects the wires coming from different branches. In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the collision point.

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 connects segments of a LAN.

Active Hubs
An active hub is actually a multipart repeater. It is normally used to create connections between stations in a physical star topology.

Bridges
A bridge 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 a table used in filtering decision.

Two-layer switch is a bridge, a bridge with many ports and a design that allows better (faster) performance. A bridge with a few ports can connect a few LANs together. A bridge with many ports may be able to allocate a unique port to each station, with each station on its own independent entity.

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.

Three-Layer Switche is a router, but a faster and more sophisticated. The switching fabric in a three-layer switch allows faster table lookup and forwarding.

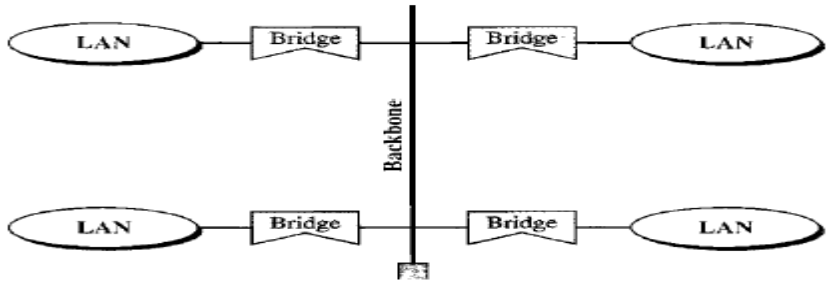
Gateway is normally a computer that operates in all five layers of the Internet or seven layers of OSI model. A gateway takes an application message, reads it, and interprets it. This means that it can be used as a connecting device between two internetworks that use different models.

Backbone Network

A backbone network allows several LANs to be connected. In a backbone network, no station is directly connected to the backbone; the stations are part of a LAN, and the backbone connects the LANs. The backbone is itself a LAN

Bus Backbone

In a bus backbone, the topology of the backbone is a bus. Bus backbones are normally used as a distribution backbone to connect different buildings in an organization. Each building can comprise either a single LAN or another backbone (normally a star backbone). A good example of a bus backbone is one that connects single- or multiple-floor buildings on a campus. Each single-floor building usually has a single LAN. Each multiple-floor building has a backbone (usually a star) that connects each LAN on a floor. A bus backbone can interconnect these LANs and backbones.



Star Backbone

In a star backbone, sometimes called a collapsed or switched backbone, the topology of the backbone is a star. In this configuration, the backbone is just one switch (that is why it is called, erroneously, a collapsed backbone) that connects the LANs. Star backbones are mostly used as a distribution backbone inside a building.