UNIT – 1

INTRODUCTION AND PHYSICAL LAYER

Networks – Network Types – Protocol Layering – TCP/IP Protocol suite – OSI Model – Physical Layer: Performance – Transmission media – Switching – Circuit-switched Networks – Packet Switching.

1.1 INTRODUCTION TO COMPUTER NETWORKS

Data Communication: When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance.

Components:

A data communications system has five components.

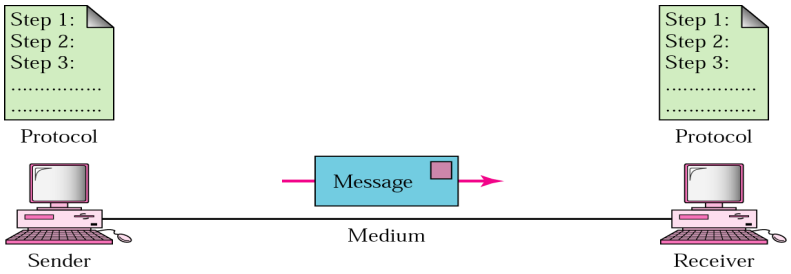


Fig. 1.1: Components of Network.

(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. 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.

Data Representation:

Information today comes in different forms such as text, numbers, images, audio, and video.

Text:

In data communications, text is represented as a bit pattern, a sequence of bits (0s or 1s). Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding. Today, the prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world. The American Standard Code for Information Interchange (ASCII), developed some decades ago in the United States, now constitutes the first 127 characters in Unicode.

Numbers:

Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations.

Images:

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution.

For example, an image can be divided into 1000 pixels or 10,000 pixels. In the second case, there is a better representation of the image (better resolution), but more memory is needed to store the image.

After an image is divided into pixels, each pixel is assigned a bit pattern. The size and the value of the pattern depend on the image. For an image made of only black and white dots (e.g., a chessboard), a 1-bit pattern is enough to represent a pixel. If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include gray scale.

For example, to show four levels of gray scale, you can use 2-bit patterns. A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10, and a white pixel by 11. There are several methods to represent color images. One method is called RGB, so called because each color is made of a combination of three primary colors: red, green, and blue. The intensity of each color is measured, and a bit pattern is assigned to it.

Audio:

Audio refers to the recording or broadcasting of sound or music.

Audio is by nature different from text, numbers, or images. It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal.

Video:

Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion. Again we can change video to a digital or an analog signal.

Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex as shown following Figures.

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 (see in the Figure 1.5). 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.

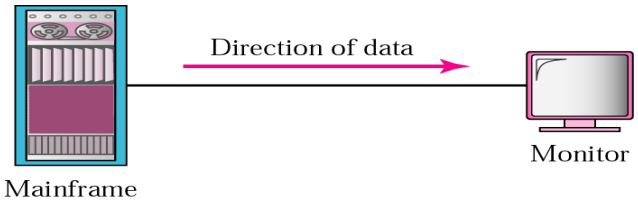


Fig. 1.5: Simplex

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.

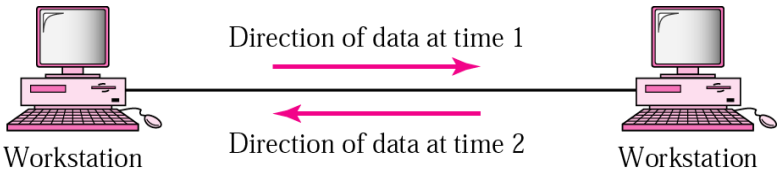


Fig. 1.6: Half Duplex

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 (see in the following Figure 1.7). 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; or the capacity of the channel is divided between signals traveling in both directions.

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.

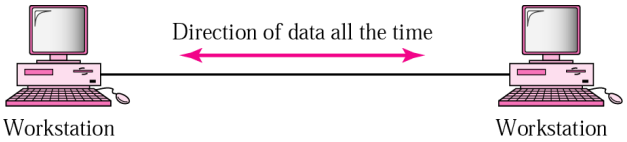


Fig. 1.7: Half Duplex

1.2 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.

Distributed Processing

Most networks use distributed processing, in which a task is divided among multiple computers. Instead of one single large machine being responsible for all aspects of process, separate computers (usually a personal computer or workstation) handle a subset.

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. We often need more throughputs and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of

traffic congestion in the network.

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, and the network's robustness in a catastrophe.

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.

Physical Structures:

Type 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
- 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.

Ex: Television channels and infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

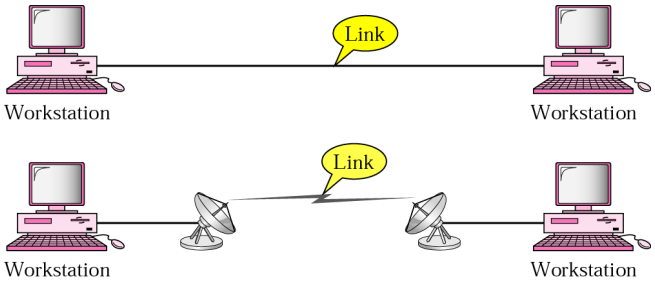


Fig : Point to point

Multipoint

A multipoint (also called multi-drop) 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.

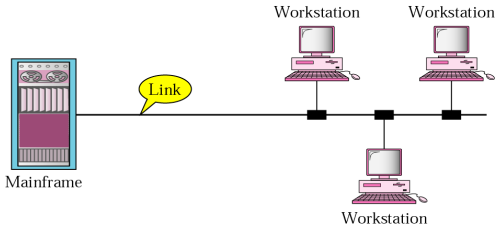


Fig: Multipoint

1.2.1 Topology

The term physical topology refers to the way in which a network is laid out physically. One or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible:

(1) Star

(2) Bus

(3) Ring

(4) Mesh

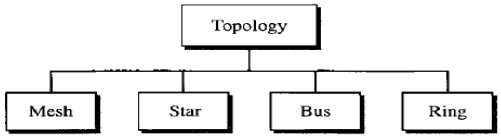


Fig : Four basic topologies

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, 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.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 ports to be connected to the other n - 1 stations.

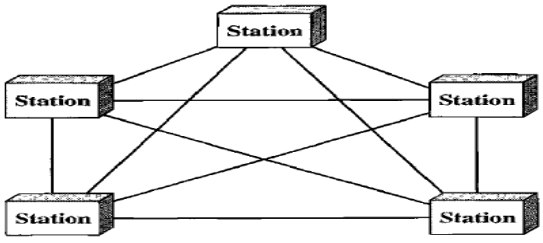


Fig: Mesh topology

Advantages:

(1) 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.

(2) A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.

(3) Privacy 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.

(4) Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems.

Disadvantages:

(1) Disadvantage of a mesh are related to the amount of cabling because every device must be connected to every other device, installation and reconnection are difficult.

(2) Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.

(3) The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

Star Topology

All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub. The hub device can be any of the following:

- Layer-1 device such as hub or repeater
- Layer-2 device such as switch or bridge
- Layer-3 device such as router or gateway

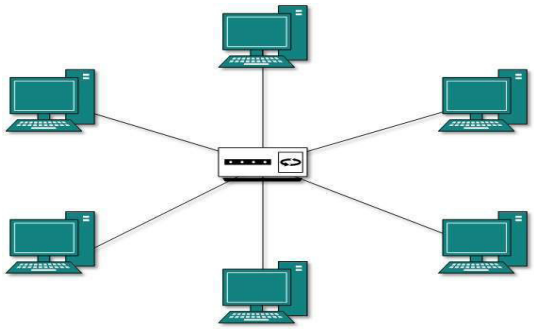


Fig.: Star Topology

Advantage

(1) Each device has a dedicated point-to-point link only

(2) Star topology does not allow direct traffic between devices

(3) Less expensive than a mesh topology

(4) Each device needs only one link and one I/O port to connect it

(5) Easy to install and reconfigure

(6) Less cable required

(7) Robustness. If one link fails, only that link is affected. All other links remain active.

(8) Easy fault identification and fault isolation

Bus Topology:

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

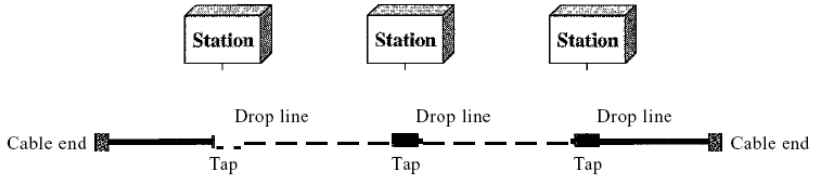


Fig: Bus topology

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 of a cable to create a contact with the metallic core.

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.

Advantage:

(1) Ease of installation.

(2) Less cable

Disadvantage:

(1) Difficult reconnection and fault isolation.

(2) Difficult to add new devices.

(3) Signal reflection at the taps can cause degradation in quality.

(4) Fault or break in the bus cable stops all transmission

(5) 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 and passes them along

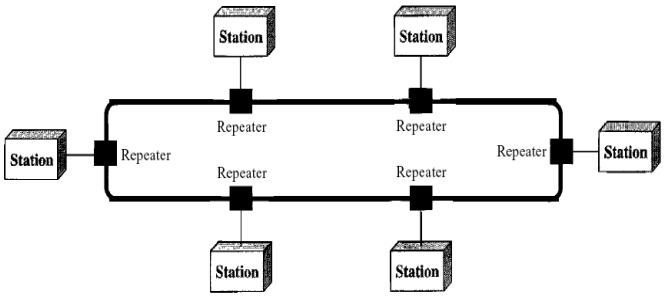


Fig: Ring topology

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. 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. Ring topology was prevalent when IBM introduced its local-area network Token Ring. Today, the need for higher-speed LANs has made this topology less popular.

1.3 CATEGORIES OF NETWORKS

Following some common types of area networks are:

- **LAN** - Local Area Network.
- **WAN** - Wide Area Network.
- **MAN** - Metropolitan Area Network.
- **WLAN** - Wireless Local Area Network.
- **SAN** - Storage Area Network, System Area Network, Server Area Network, or sometimes Small Area Network.
- **CAN** - Campus Area Network, Controller Area Network, or sometimes Cluster Area Network.
- **PAN** - Personal Area Network.

1.3.1 Local Area Network:

Local area networks, generally called LANs, are privately-owned networks within a single building or campus of up to a few kilometers in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information. LANs are distinguished from other kinds of networks by three characteristics:

(1) Their size,

(2) Their transmission technology, and

(3) Their topology.

LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance. Knowing this bound makes it possible to use certain kinds of designs that would not otherwise be possible. It also simplifies network management.

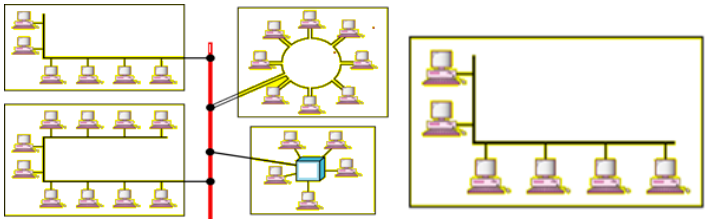


Fig: Local area networks

LANs may use a transmission technology consisting of a cable to which all the machines are attached, like the telephone company party lines once used in rural areas. Traditional LANs run at speeds of 10 Mbps to 100 Mbps, have low delay (microseconds or nanoseconds), and make very few errors. Newer LANs operate at up to 10 Gbps various topologies are possible for broadcast LANs. Figure1 shows two of them. In a bus (i.e., a linear cable) network, at any instant at most one machine is the master and is allowed to transmit. All other machines are required to refrain from sending. An arbitration mechanism is needed to resolve conflicts when two or more machines want to transmit simultaneously. The arbitration mechanism may be centralized or distributed. IEEE 802.3, popularly called Ethernet, for example, is a bus-based broadcast network with decentralized control, usually operating at 10 Mbps to 10 Gbps. Computers on an Ethernet can transmit whenever they want to; if two or more packets collide, each computer just waits a random time and tries again later.

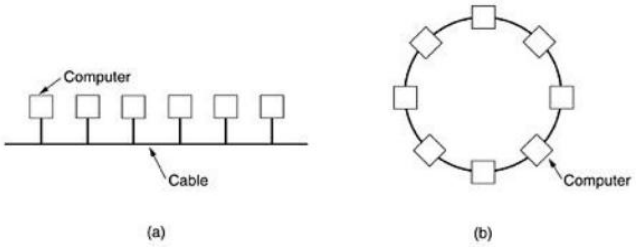


Fig.: Two broadcast networks. (a) Bus. (b) Ring.

A second type of broadcast system is the ring. In a ring, each bit propagates around on its own, not waiting for the rest of the packet to which it belongs. Typically, each bit circumnavigates the entire ring in the time it takes to transmit a few bits, often before the complete packet has even been transmitted. As with all other broadcast systems, some rule is needed for arbitrating simultaneous accesses to the ring. Various methods, such as having the machines take turns, are in use. IEEE 802.5 (the IBM token ring), is a ring-based LAN operating at 4 and 16 Mbps. FDDI is another example of a ring network.

1.3.2 Metropolitan Area Network (MAN)

A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable television network available in many cities. This system grew from earlier community antenna systems used in areas with poor over-the-air television reception. In these early systems, a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers' houses. At first, these were locally-designed, ad hoc systems. Then companies began jumping into the business, getting contracts from city governments to wire up an entire city. The next step was television programming and even entire channels designed for cable only. Often these channels were highly specialized, such as all news, all sports, all cooking, all gardening, and so on. But from their inception until the late 1990s, they were intended for television reception only. To a first approximation, a MAN might look something like the system shown in Figure 1.17. In this figure both television signals and Internet are fed into the centralized head end for subsequent distribution to people's homes. Cable television is not the only MAN. Recent developments in high-speed wireless Internet access resulted in another MAN, which has been standardized as IEEE 802.16.

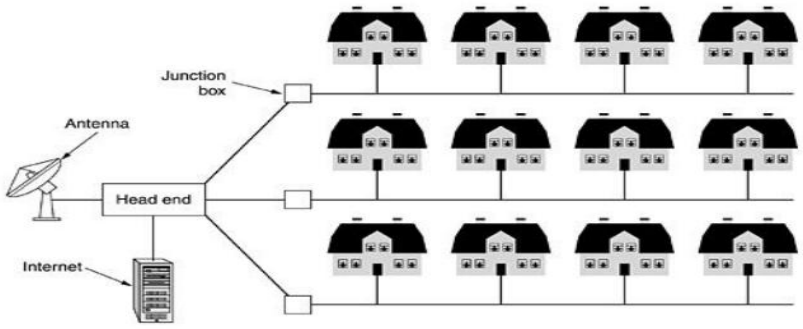


Fig: Metropolitan area network based on cable TV.

A MAN is implemented by a standard called DQDB (Distributed Queue Dual Bus) or IEEE 802.16. DQDB has two unidirectional buses (or cables) to which all the computers are attached.

1.3.3 Wide Area Network (WAN)

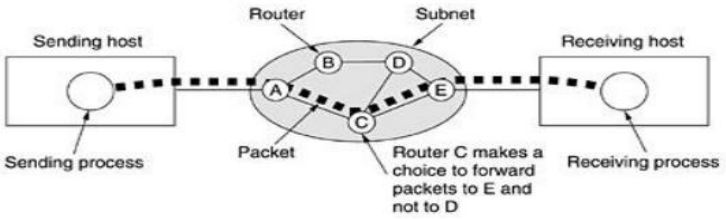
A wide area network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user (i.e., application) programs. These machines are called as hosts. The hosts are connected by a communication subnet, or just subnet for short. The hosts are owned by the customers (e.g., people's personal computers), whereas the communication subnet is typically owned and operated by a telephone company or Internet service provider. The job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener.

Separation of the pure communication aspects of the network (the subnet) from the application aspects (the hosts), greatly simplifies the complete network design. In most wide area networks, the subnet consists of two distinct components: transmission lines and switching elements. Transmission lines move bits between machines. They can be made of copper wire, optical fiber, or even radio links. In most WANs, the network contains numerous transmission lines, each one connecting a pair of routers. If two routers that do not share a transmission line wish to communicate, they must do this indirectly, via other routers.

When a packet is sent from one router to another via one or more intermediate routers, the packet is received at each intermediate router in its entirety, stored there until the required output line is free, and then forwarded. A subnet organized according to this principle is called a store-and-forward or packet-switched subnet. Nearly all wide area networks (except those using satellites) have store-and-forward subnets. When the packets are small and all the same size, they are often called cells.

The principle of a packet-switched WAN is so important. Generally, when a process on some host has a message to be sent to a process on some other host, the sending host first cuts the message into packets, each one bearing its number in the sequence. These packets are then injected into the network one at a time in quick succession. The packets are transported individually over the network and deposited at the receiving host, where they are reassembled into the original message and delivered to the receiving process. A stream of packets resulting from some initial message is illustrated in Figure

In this figure, all the packets follow the route ACE, rather than ABDE or ACDE. In some networks all packets from a given message must follow the same route; in others each packed is routed separately of course, if ACE is the best route, all packets may be sent along it, even if each packet is individually routed.



Not all WANs are packet switched. A second possibility for a WAN is a satellite system. Each router has an antenna through which it can send and receive. All routers can hear the output from the satellite, and in some cases, they can also hear the upward transmissions of their fellow routers to the satellite as well. Sometimes the routers are connected to a substantial point-to-point subnet, with only some of them having a satellite antenna.

A network must be able to meet certain criteria, these are mentioned below:

(1) Performance.

(2) Reliability.

(3) Scalability.

Performance

It can be measured in the following ways:

- **Transit time: It** is the time taken to travel a message from one device to another.
- **Response time: It** is defined as the time elapsed between enquiry and response.

Other ways to measure performance are:

(1) Efficiency of software.

(2) Number of users.

(3) Capability of connected hardware.

Reliability

It decides the frequency at which network failure take place. More the failures are, less is the network's reliability.

Security

It refers to the protection of data from any unauthorized user or access. While travelling through network, data passes many layers of network, and data can be traced if attempted. Hence security is also a very important characteristic for Networks.

Properties of a Good Network

(1) Interpersonal Communication: We can communicate with each other efficiently and easily. Example: emails, chat rooms, video conferencing etc, all of these are possible because of computer networks.

(2) Resources can be shared: We can share physical resources by making them available on a network such as printers, scanners etc.

(3) Sharing files, data: Authorized users are allowed to share the files on the network.

Basic Communication Model

A Communication model is used to exchange data between two nodes. For example: communication between a computer, server and telephone (through modem).

Fig.: Communication model

Sender

Data to be transmitted is generated by this device, example: telephones, personal computers etc.

Transmitter

The data generated by the source system is not directly transmitted in the form its generated. The transmitter transforms and encodes the data in such a form to produce electromagnetic waves or signals.

Transmission System

A transmission system can be a single transmission line or a complex network connecting source and destination.

Receiver

Receiver accepts the signal from the transmission system and converts it into a form which is easily managed by the destination device.

Destination

Destination receives the incoming data from the receiver.

Uses of Computer Networks

Business Applications

- **Resource Sharing:** The goal is to make all programs, equipments, and especially data, available to anyone on the network without regard to the physical location of the resource and the user.
- **Server-Client model:** One can imagine a company's information system as consisting of one or more databases and some number of employees who need to access them remotely. In this model, the data is stored on powerful computers called **servers**. Often these are centrally housed and maintained by a system administrator. In contrast, the employees have simple machines, called **clients**, on their desks, with which they access remote data.
- **Communication Medium:** A computer network can provide a powerful communication medium among employees. Virtually every company that has two or more computers now has e-mail (electronic mail), which employees generally use for a great deal of daily communication.
- **E-Commerce:** A goal that is starting to become more important is doing business with consumers over the Internet. Airlines, bookstores and music vendors have discovered that many customers like the convenience of shopping from home. This sector is expected to grow quickly in the future. The most popular forms are listed in the below figure:

Tag and Full Name	Example
B2C Business to consumer	Ordering Books online
B2B business to Business	Car manufacturer ordering tires from supplier
C2C Consumer to consumer	Auctioning second –hand products online
G2C Government to consumer	Government distributing tax forms electronically
P2P Peer to peer	File Sharing

Table.Most popular forms

Home Applications

Some of the most important uses of the Internet for home users are as follows:

- Access to remote information.
- Person-to-person communication.

- Interactive entertainment.
- Electronic commerce.

Mobile Users

Mobile computers, such as notebook computers and Mobile phones, are one of the fastest-growing segments of the computer industry. Although wireless networking and mobile computing are often related, they are not identical, as the below table 2 shows.

Wireless	Mlobile	Applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in older, unwired buildings
Yes	Yes	Portable office; PDA for store inventory

Table.2: Mobile User

1.4 PROTOCOL LAYERING

1.4.1 Protocols:

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

- **Syntax**. The term syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.
- **Semantics**. The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?
- **Timing**. The term timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

Layered Tasks

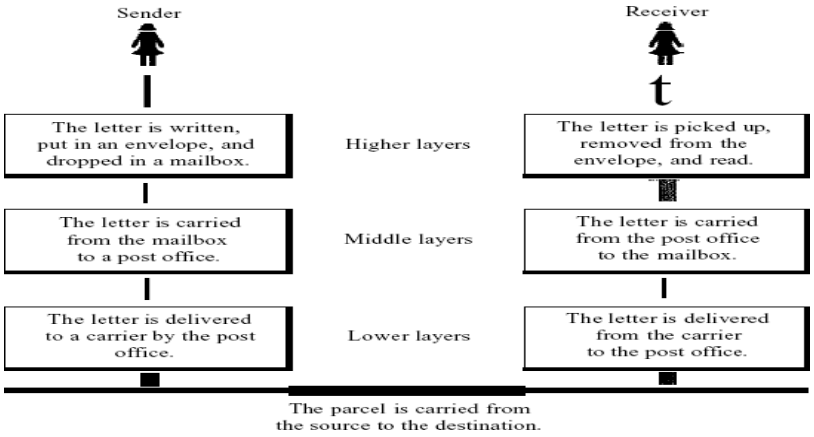


Fig : Protocol Layering

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail. The process of sending a letter to a friend would be complex if there were no services available from the post office. Below Figure shows the steps in this task.

1.5 TCP/IP REFERENCE MODEL

Introduction to TCP/IP REFERENCE Model

TCP/IP is transmission control protocol and internet protocol. Protocols are set of rules which govern every possible communication over the internet. These protocols describe the movement of data between the host computers or internet and offers simple naming and addressing schemes.

CP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. Protocols are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. These protocols offer simple naming and addressing schemes.

Overview of TCP/IP reference model

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defense's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

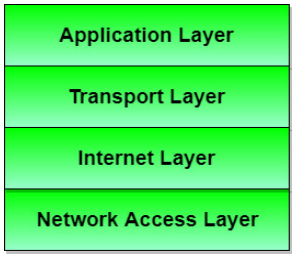


Figure.1.32: interaction between layers

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact until the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

Description of different TCP/IP protocols

Layer 1: Host-to-network Layer

(1) Lowest layer of the all.

(2) Protocol is used to connect to the host, so that the packets can be sent over it.

(3) Varies from host to host and network to network.

Layer 2: Internet layer

(1) Selection of a packet switching network which is based on a connectionless internetwork layer is called an internet layer.

(2) It is the layer which holds the whole architecture together.

(3) It helps the packet to travel independently to the destination.

(4) Order in which packets are received is different from the way they are sent.

(5) IP (Internet Protocol) is used in this layer.

Layer 3: Transport Layer

(1) It decides if data transmission should be on parallel path or single path.

(2) Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.

(3) The applications can read and write to the transport layer.

(4) Transport layer adds header information to the data.

(5) Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

(6) Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

(1) TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.

(2) FTP (File Transfer Protocol) is a protocol that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.

(3) SMTP (Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.

(4) DNS (Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.

Merits of TCP/IP model

(1) It operated independently.

(2) It is scalable.

(3) Client/server architecture.

(4) Supports a number of routing protocols.

(5) Can be used to establish a connection between two computers.

Demerits of TCP/IP

(1) In this, the transport layer does not guarantee delivery of packets.

(2) The model cannot be used in any other application.

(3) Replacing protocol is not easy.

(4) It has not clearly separated its services, interfaces and protocols.

1.6 INTRODUCTION TO ISO-OSI MODEL

OSI Architecture

ISO defines a common way to connect computer by the architecture called Open System Interconnection (OSI) architecture. Network functionality is divided into seven layers.

(1) Application layer – establishes interface between a user and a host computer, e.g., searching in a database application.

(2) Presentation layer – determines syntactic representation of data, e.g., agreement on character code like ASCII/Unicode.

(3) Session layer – creates and manages sessions when one application process requests access to another applications process

(4) Transport layer – deals with data transfer between end systems and determines flow control.

(5) Network layer – establishes paths for data between computers and determines switching among routes between computers, determines how to disaggregate messages into individual packets.

(6) Physical layer – controls electrical and mechanical aspects of data transmission, e.g., voltage levels, cable lengths, and so on.

(7) Data-link layer – addresses the transmission of data frames (or packets) over a physical link **between** network entities, includes error correction.

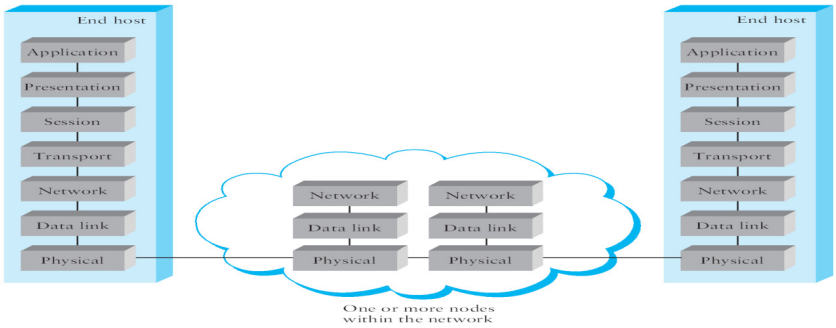


Figure: OSI layers

Organization of the layers

The 7 layers can be grouped into 3 subgroups

(1) Network Support Layers

Layers 1, 2, 3 - Physical, Data link and Network are the network support layers. They deal with the physical aspects of moving data from one device to another such as electrical specifications, physical addressing, transport timing and reliability.

(2) Transport Layer

Layer4, transport layer, ensures end-to-end reliable data transmission on a single link.

(3) User Support Layers

Layers 5,6,7 – Session, presentation and application are the user support layers. They allow interoperability among unrelated software systems. A Data exchange using the OSI model

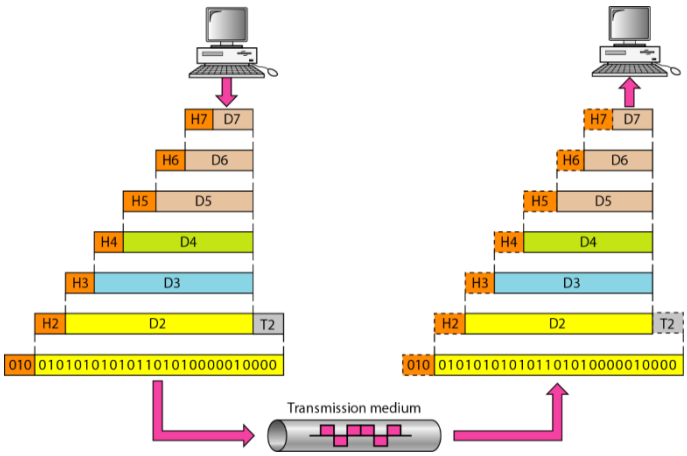


Figure.1.22: Data exchange using the OSI model

Functions of the Layers

(1) Physical Layer

The physical layer coordinates the functions required to transmit a bit stream over a physical medium.

The physical layer is concerned with the following:

- **Physical characteristics of interfaces and media** - The physical layer defines the characteristics of the interface between the devices and the transmission medium.
- **Representation of bits** - To transmit the stream of bits, it must be encoded to signals. The physical layer defines the type of encoding.

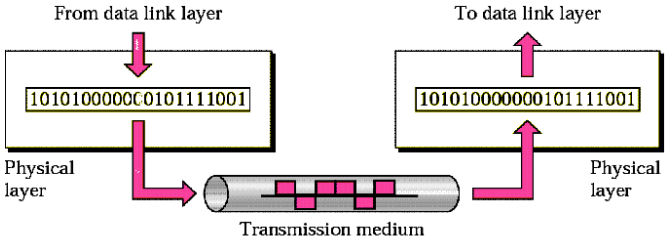


Figure.Physical layer

- **Data Rate or Transmission rate** - The number of bits sent each second – is also defined by the physical layer.
- **Synchronization of bits** - The sender and receiver must be synchronized at the bit level. Their clocks must be synchronized.
- **Line Configuration** - 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, bus, and star or ring topology.
- **Transmission Mode -** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex or full-duplex.

(2) Data Link Layer

It is responsible for transmitting frames from one node to next node.

The other responsibilities of this layer are

- **Framing** - Divides the stream of bits received into data units called frames.
- **Physical addressing** – If frames are to be distributed to different systems on the n/w , data link layer adds a header to the frame to define the sender and receiver.

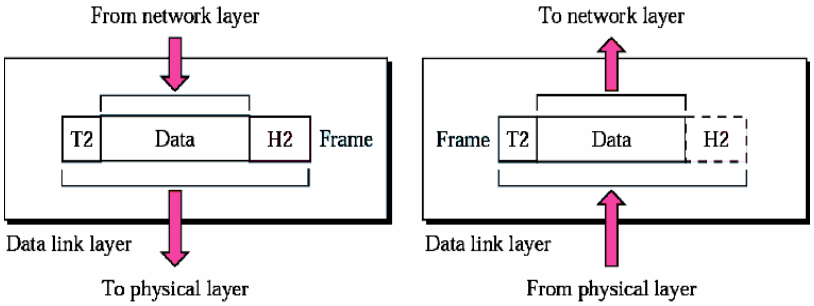


Figure : Data link layer

- **Flow control-** If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender, the Data link layer imposes a flow ctrl mechanism.
- **Error control-** Used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.
- **Access control -**Used to determine which device has control over the link at any given time.

(3) Network Layer

This layer is responsible for the delivery of packets from source to destination.

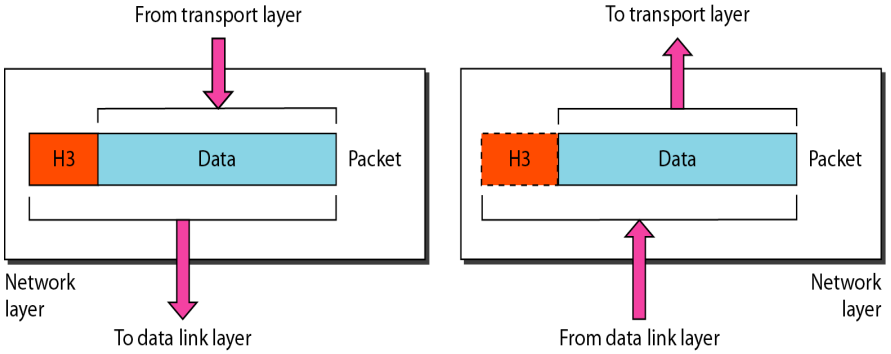


Figure : Network layer

It is mainly required, when it is necessary to send information from one network to another. The other responsibilities of this layer are

- **Logical addressing** - If a packet passes the n/w boundary, we need another addressing system for source and destination called logical address.
- **Routing** – The devices which connects various networks called routers are responsible for delivering packets to final destination.

(4) Transport Layer

- It is responsible for Process to Process delivery.
- It also ensures whether the message arrives in order or not.

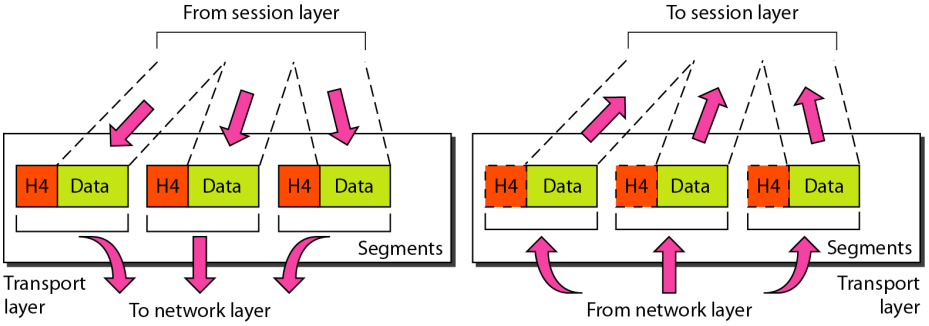


Figure.Transport layer

The other responsibilities of this layer are

- **Port addressing** - The header in this must therefore include a address called port address. This layer gets the entire message to the correct process on that computer.
- **Segmentation and reassembly** - The message is divided into segments and each segment is assigned a sequence number. These numbers are arranged correctly on the arrival side by this layer.
- **Connection control** - This can either be connectionless or connection-oriented. The connectionless treats each segment as a individual packet and delivers to the destination. The connection-oriented makes connection on the destination side before the delivery. After the delivery the termination will be terminated.
- **Flow and error control -** Similar to data link layer, but process to process take place.

(5) Session Layer

This layer establishes, manages and terminates connections between applications.

The other responsibilities of this layer are

- **Dialog control** - This session allows two systems to enter into a dialog either in half duplex or full duplex.
- **Synchronization**-This allows to add checkpoints into a stream of data.

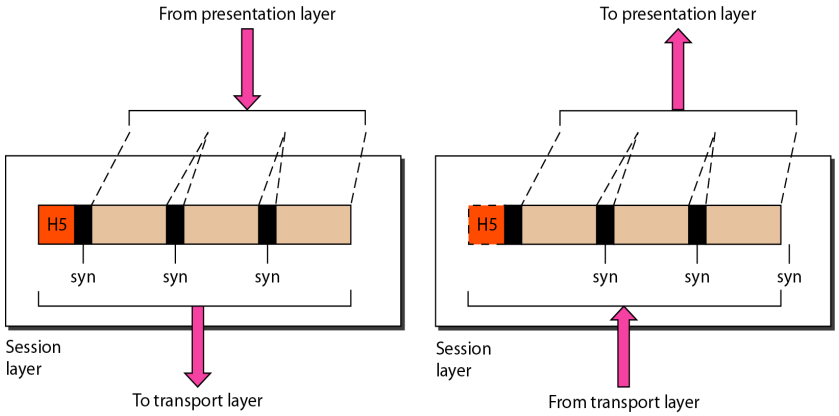


Figure.Session layer

(6) Presentation Layer

It is concerned with the syntax and semantics of information exchanged between two systems.

The other responsibilities of this layer are

- **Translation** – Different computers use different encoding system, this layer is responsible for interoperability between these different encoding methods. It will change the message into some common format.

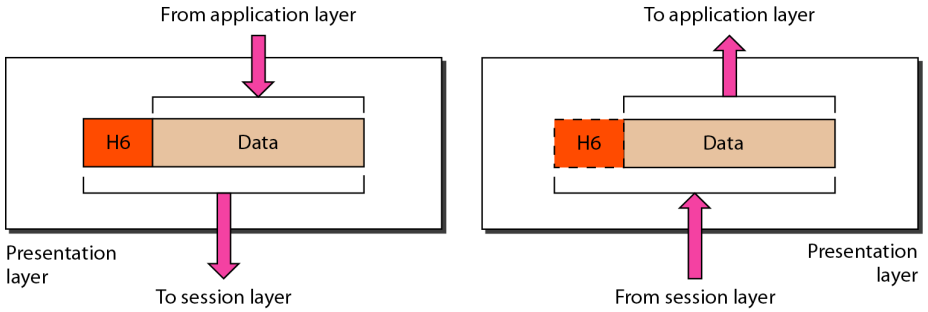


Figure: Transport layer

- **Encryption and decryption**-It means that sender transforms the original information to another form and sends the resulting message over the n/w. and vice versa.
- **Compression and expansion –** Compression reduces the number of bits contained in the information particularly in text, audio and video.

(7) Application Layer

This layer enables the user to access the network. This allows the user to log on to remote user.

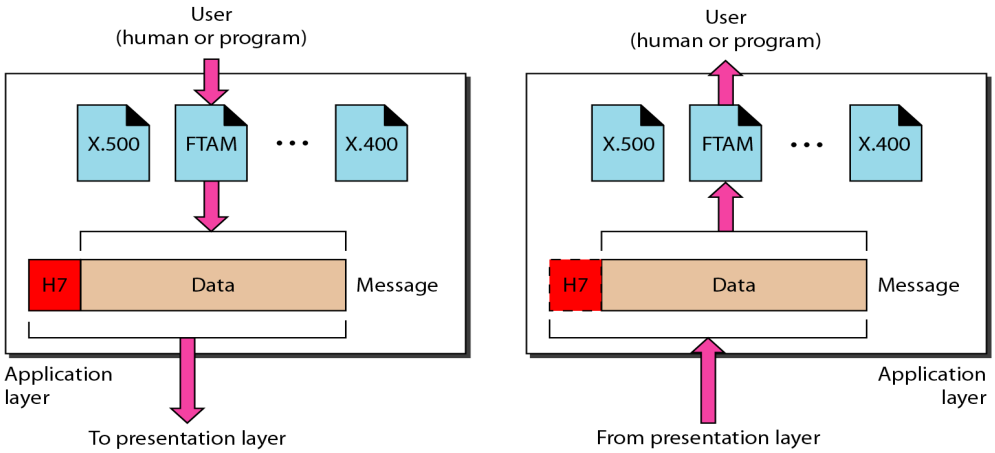


Figure: Transport layer

The other responsibilities of this layer are

- FTAM (file transfer, access, mgmt) - Allows user to access files in a remote host.
- Mail services - Provides email forwarding and storage.
- Directory services - Provides database sources to access information about various sources and objects.

Summary of layers

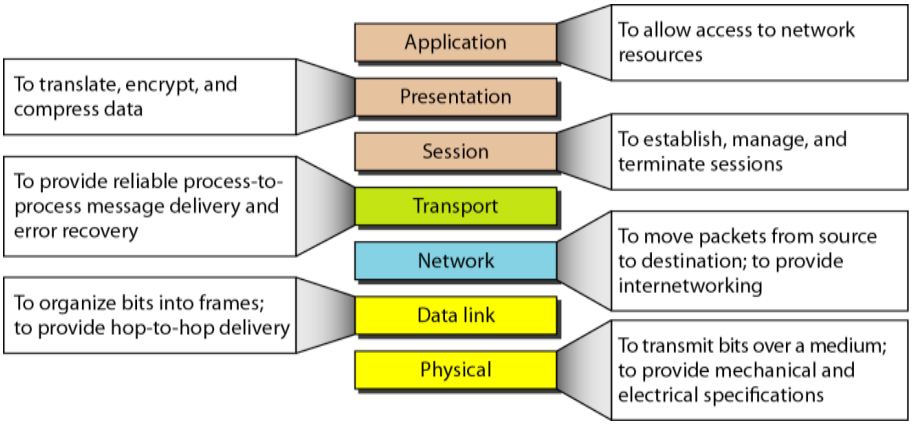


Figure: Summary of layer

The interaction between layers in the OSI model

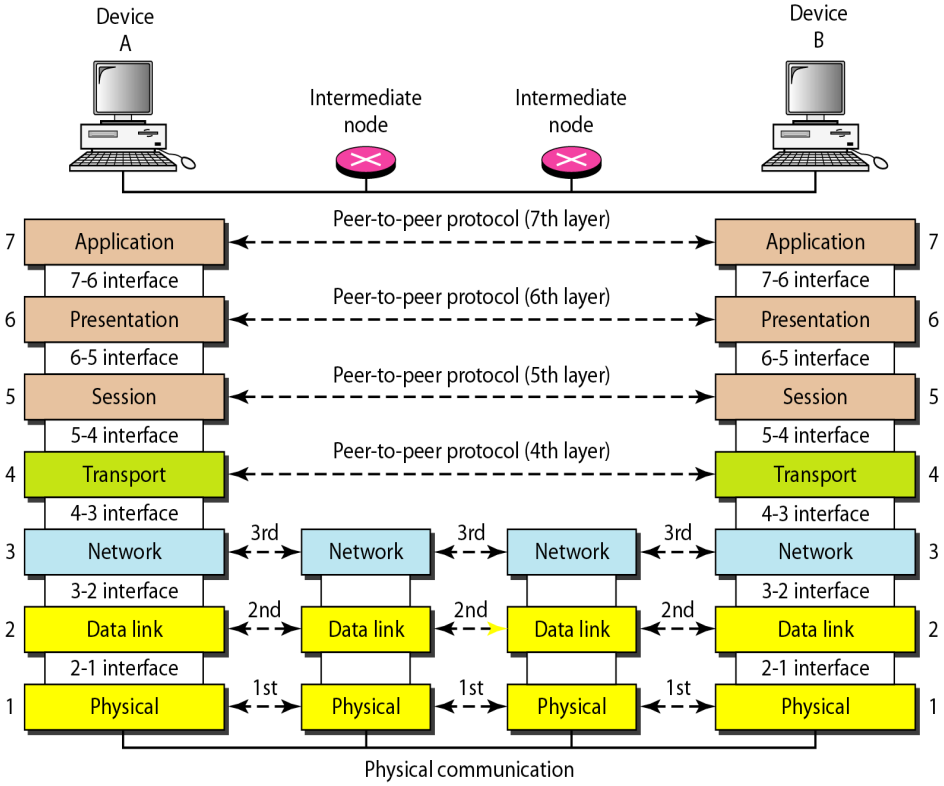


Figure: interaction between layers

Comparison of OSI Reference Model and TCP/IP Reference Model

Following are some major differences between OSI Reference Model and TCP/IP Reference Model, with diagrammatic comparison below.

OSI (Open System Interconnection)	TCP/IP (Transmission Control Protocol / Internet Protocol)
1) OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1) TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2) In OSI model the transport layer guarantees the delivery of packets.	2) In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3) Follows vertical approach.	3) Follows horizontal approach.
4) OSI model has a separate Presentation layer and Session layer.	4) TCP/IP does not have a separate Presentation layer or Session layer.
5) OSI is a reference model around which the networks are built. Generally, it is used as a guidance tool.	5) TCP/IP model is, in a way implementation of the OSI model.
6) Network layer of OSI model provides both connection oriented and connectionless service.	6) The Network layer in TCP/IP model provides connectionless service.
7) OSI model has a problem of fitting the protocols into the model.	7) TCP/IP model does not fit any protocol
8) Protocols are hidden in OSI model and are easily replaced as the technology changes.	8) In TCP/IP replacing protocol is not easy.
9) OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	9) In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
10) It has 7 layers	10) It has 4 layers

1.7 PHYSICAL LAYER

Physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit, it is recieved by the other side as 1 bit and not as 0 bit. In physical layer we deal with the communication medium used for transmission.

Transmission media is a pathway that carries the information from sender to receiver. We use different types of cables or waves to transmit data. Data is transmitted normally through electrical or electromagnetic signals.

An electrical signal is in the form of current. An electromagnetic signal is series of electromagnetic energy pulses at various frequencies. These signals can be transmitted through copper wires, optical fibers, atmosphere, water and vacuum Different Medias have different

properties like bandwidth, delay, cost and ease of installation and maintenance. Transmission media is also called **Communication channel.**

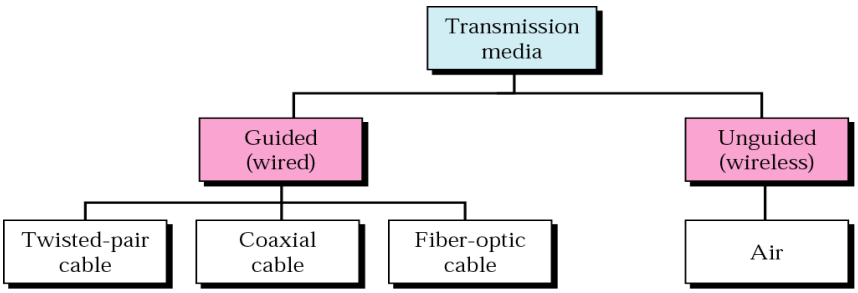


Figure: Classification of Transmission media

1.7.1 Guided Media

Guided media conduct signals from one device to another include Twisted-pair cable, Coaxial Cable and Fiber-optic cable. 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 glass cable that accepts and transports signals in the form of light.

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.
- Other is used as ground reference.

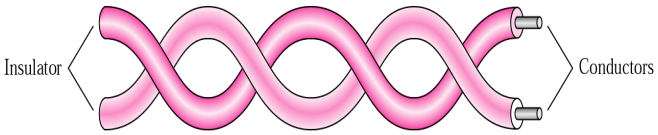


Figure : Twisted pair cables

Interference and cross talk may affect both the wires and create unwanted signals, if the two wires are parallel.

By twisting the pair, a balance is maintained. Suppose in one twist one wire is closer to noise and the other is farther in the next twist the reverse is true. Twisting makes it probable that both wires are equally affected by external influences.

Twisted Pair Cable comes into two forms:

- **Unshielded.**
- **Shielded.**

Unshielded versus shielded Twisted-Pair Cable

- Shielded Twisted-Pair (STP) Cable has a metal foil or braided-mesh covering that encases each pair of insulated conductors.

- Metal casing improves that quality of cable by preventing the penetration of noise or cross talk.
- It is more expensive. The following figure shows the difference between UTP and STP.

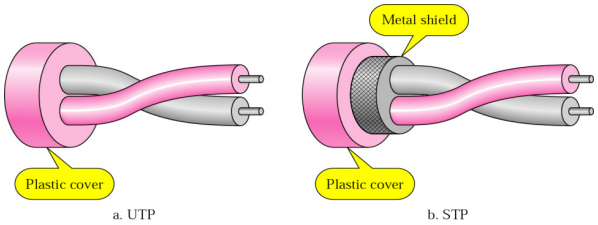


Figure : Unshielded versus shielded Twisted-Pair Cable

Applications

- Twisted Pair cables are used in telephone lines to provide voice and data channels.
- Local area networks also use twisted pair cables.

Coaxial Cable

Coaxial cable (coax) carries signals of higher frequency ranges than 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, and with outer conductor of metal foil. The outer metallic wrapping serves both as a shield against noise and as the second conductor and the whole cable is protected by a plastic cover.

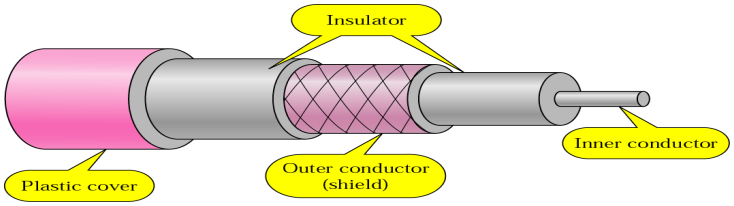


Figure : Coaxial cable

Categories of coaxial cables

Category	Impedance	Use
RG-59	75	Cable TV
RG-58	50	Thin Ethernet
RG-11	50	Thick Ethernet

Table: Categories of coaxial cables

Coaxial cables come in two types:

a) **Baseband:** Transmission of single signal at high speed.

b) **Broadband:** Transmission of many signals simultaneously.

Baseband Coaxial cable:

- It is used for digital transmission and It is mostly used for LAN's.
- Baseband transmits a single signal at a time with very high speed.

Broadband Coaxial cable:

- This uses analog transmission on standard cable television cabling.
- It transmits several simultaneous signal using different frequencies.
- It covers large area when compared with Baseband Coaxial Cable.

Applications

- It is used in analog and digital telephone networks.
- It is also used in Cable TV networks.
- It is used in Ethernet LAN.

Connectors

- ***BNC connector*** – to connect the end of the cable to a device.
- ***BNC T*** - to branch out network connection to computer.
- ***BNC terminator*** - at the end of the cable to prevent the reflection of the signal.

Fiber Optic Cable

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

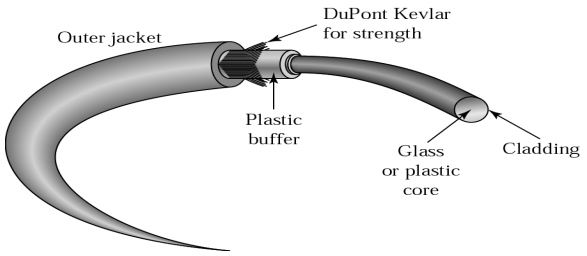


Figure : Fiber-optic cable

Properties of light travel in a straight line as long as it moves through a single uniform substance. If traveling through one substance suddenly enters another, ray changes its direction.

Refraction and Reflection

- Refraction often occurs when light bends as it passes from one medium to another less dense medium.
- When this angle results in a refraction great enough, reflection occurs and the light no longer passes into the less dense medium.

Reflection

- Optical fibers use reflection to guide light through a channel.

- Information is encoded onto a beam of light as a series of on-off pulses representing 1s and 0s.

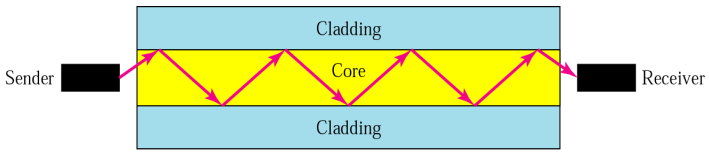


Figure : Fiber-optic cable

Propagation Modes

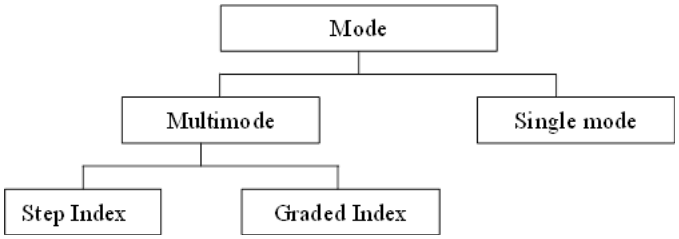


Figure : Propagation Modes

Multimode

In the multiple mode, multiple light beams from a source move through the core in different paths.

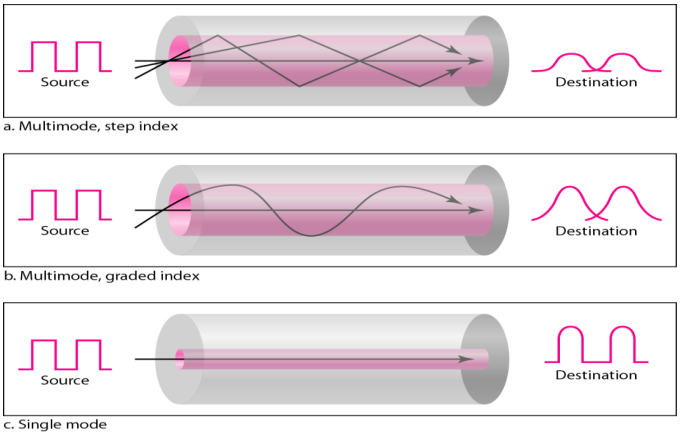


Figure : Propagation Modes

- ***Multimode-Step-Index fiber:*** The density of core remains constant from the centre to the edge. A ray of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface there is an abrupt change to a lower density that changes the angle of the beam's motion.
- ***Multimode- Graded -Index fiber:*** The density is varying. Density is highest at the centre of the core and decreases gradually to its lowest at the edge.
- ***Single Mode*** Single mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single mode fiber itself is manufactured with a much smaller diameter than that of multimedia fiber.

Applications of Fiber Optics

- Backbone networks due to wide bandwidth and cost effectiveness.
- Cable TV.
- LANS.
  - 100Base-FX (Fast Ethernet).
  - 1000Base-X.

Advantages of Fiber Optics

- Higher bandwidth than twisted-pair and coaxial cable; not limited by medium, but by equipment used to generate and receive signals.
- Noise resistance..
- Less signal attenuation.
- More resistant to corrosive materials.
- Lightweight.
- Greater security.

Disadvantages of Fiber Optics

- Installation/maintenance.
- Unidirectional.
- Cost.

Connectors

- **Subscriber channel** (SC) **connector** is used for cable TV.
- **Straight-tip** (ST) **connector** is used for connecting cable to networking devices.

Advantages of Optical Fiber

- Noise resistance.
- Less signal attenuation.
- Light weight.

Disadvantages

- Cost.
- Installation and maintenance.
- Unidirectional.
- Fragility (easily broken).

Advantages of Twisted pair cable

- It can be used to carry both analog and digital data.
- It is relatively easy to implement and terminate.
- It is the least expensive media of transmission for short distances.
- If portion of a twisted pair cable is damaged it does not affect the entire network.

Disadvantages of Twisted pair cable

- Attenuation is very high.
- It supports lower bandwidth as compared to other Medias. It supports 10 mbps up to a distance of 100 meters on a 10BASE-T.
- It offers very poor security and is relatively easy to tap.
- Being thin in size, they are likely to break easily.

1.7.2 Unguided Media

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

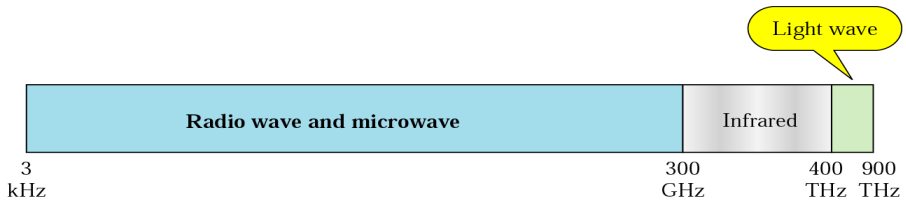


Figure : Transmission range of unguided media

Wireless Propagation Methods

- Ground – radio waves travel through lowest portion of atmosphere, hugging the Earth.
- Sky – higher-frequency radio waves radiate upward into ionosphere and then reflect back to Earth.
- Line-of-sight – high-frequency signals transmitted in straight lines directly from antenna to antenna.

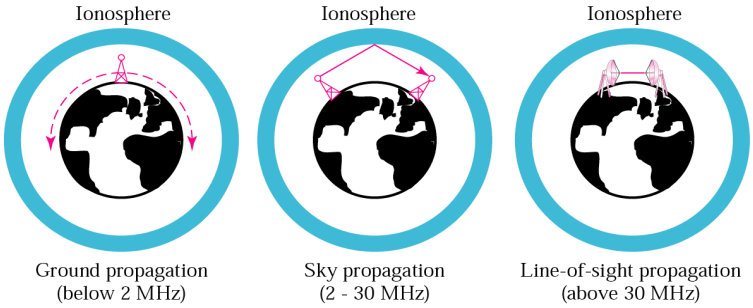


Figure : Wireless Propagation Methods

Unguided signals can travel from the source to destination in several ways:

- **Ground propagation** – waves travel through lowest portion on atmosphere.
- **Sky propagation** – High frequency waves radiate upward into ionosphere and reflected back to earth.
- **Line-of-sight propagation** – Very high frequency signals travel in a straight line

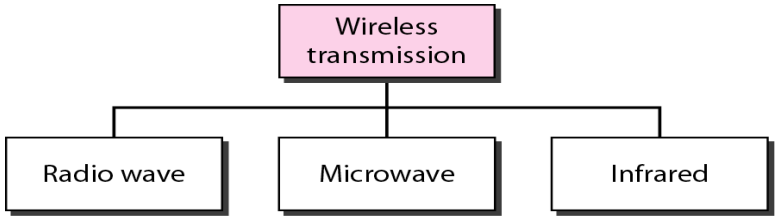


Figure : Classification of Unguided media

1.8 RADIO WAVES

Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves.

Band	Range	Propagation	Application
VLF	3–30 KHz	Ground	Long-range radio navigation
LF	30–300 KHz	Ground	Radio beacons and navigational locators
MF	300 KHz–3 MHz	Sky	AM radio
HF	3–30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF	3–30 GHz	Line-of-sight	Satellite communication
EHF	30–300 GHz	Line-of-sight	Radar, satellite communication

Table : Band and range of radio waves

Properties

- Radio waves are Omni-directional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned.
- A sending antenna sends waves that can be received by any receiving antenna.
- Radio waves, particularly those of low and medium frequencies, can penetrate walls.

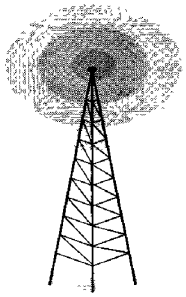


Figure : Omni-directional antenna

Disadvantages

- The Omni directional property has a disadvantage, that the radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.
- As Radio waves can penetrate through walls, we cannot isolate a communication to just inside or outside a building.

Applications

Radio waves are used for multicast communications, such as radio and television, and paging systems.

1.9 MICROWAVES

- Electromagnetic waves having frequencies between 1 and 300 GHz are called micro waves.
- Microwave is a technology for transmitting both digital and analog signals.
- Micro waves are unidirectional.
- Microwave transmission also requires line of sight in order to work properly.
- The distance covered by microwave signals is based upon the height of the antenna

Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.

Properties

- Microwaves are unidirectional.
- Sending and receiving antennas need to be aligned.
- Microwave propagation is line-of-sight
- Very high-frequency microwaves cannot penetrate walls.

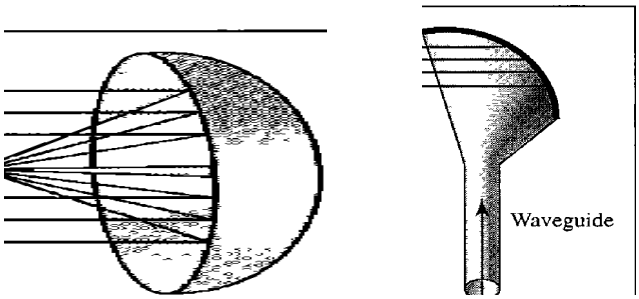


Figure.: a) Parabolic Dish antenna *Figure:b) Horn antenna*

- Parabolic Dish antenna focuses all incoming waves into single point.
- Outgoing transmissions are broadcast through a horn aimed at the dish.

Applications

- Microwaves, due to their unidirectional properties, are very useful when unicast (one-to-one) communication is needed between the sender and the receiver.
- They are used in cellular phones, satellite networks and wireless LANs.
- There are 2 types of Microwave Transmission:
  - Terrestrial Microwave.
  - Satellite Microwave.

Terrestrial Microwave

- Terrestrial microwave transmissions are sent signals between two microwave stations on the earth (earth station).
- It is the most common form of long-distance communication.
- The frequencies used are in the low-gigahertz range, which limits all communications to line-of-sight.
- It is an example of telephone systems all over the world

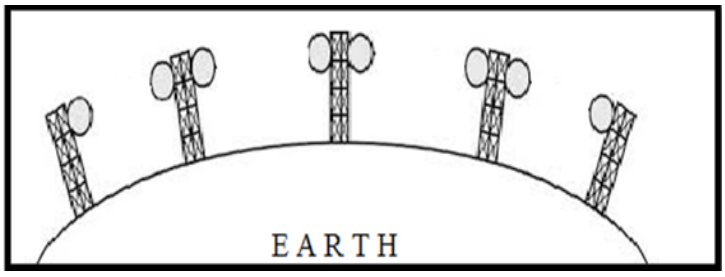


Figure : Terrestrial microwave (example of telephone systems)

Satellite Microwave

- Satellite microwave systems relay transmissions through communication satellites.
- Satellites range at this distance remains located above a fixed point on earth.

- Bandwidth capacity depends on the frequency used.
- Satellite microwave deployment for range satellite is difficult.

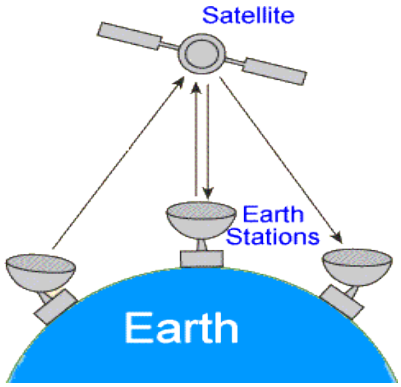


Figure : Satellite microwave systems

Advantages of Microwave Transmission

- No cables needed.
- Multiple channels available.
- Wide bandwidth.
- Used for long distance telephone communication.
- Carries 1000's of voice channels at the same time.

Disadvantages of Microwave Transmission

- It is Very costly and Towers are expensive to build.
- Signal is interrupt if any obstacle occurs.
- Microwaves suffer from decrease or loose signal due to atmospheric conditions like snow, rain, fog and storm.

1.10 INFRARED TRANSMISSION MEDIA

- Infrared transmission media is electromagnetic radiations which have frequency range between from 300 GHz to 400 THz.
- The name means Infrared, the Latin infra meaning below.
- Red is the color of the longest wavelengths of visible light.
- Infrared light has a lower frequency than that of red light visible to humans, hence the literal meaning of below red.
- It can be used for short-range communication.
- Infrared waves having high frequencies.
- It cannot go through walls.
- Prevents interference between one system and another, a short-range communication system in on room cannot be affected by another system in the next room.

- When we use infrared remote control, we do not interfere with the use of the remote by our neighbors.
- However, this same characteristic makes infrared signals useless for long-range communication.
- In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Applications of Infrared:

- Home-entertainment remote-control boxes.
- Wireless (local area networks).
- Links between notebook computers and desktop computers.
- Cordless modem.
- Fire sensors.
- Night-vision systems.
- Medical diagnostic equipment.
- Missile guidance systems.
- Geological monitoring device.

Following are the features of Infrared wireless technology:

- It is developed for point to point links between two devices for data transfer as well as file synchronization.
- It works using infrared light beams.
- It occupies 300 GHz and 400 THz frequency in optical bands.
- It covers distance of 10 to 30 meters.
- Data rate of up to 4 Mbps can be achieved.
- It supports maximum up to 2 devices.
- The main application is short range, one to one data exchange.

Advantages of Infrared

- The devices are very cheap.
- The devices are compact, lightweight and consume low power.
- The technology-based devices are easy to use.
- It is non interfering from RF waves.
- It is more secure compare to RF technologies.

Disadvantages of Infrared

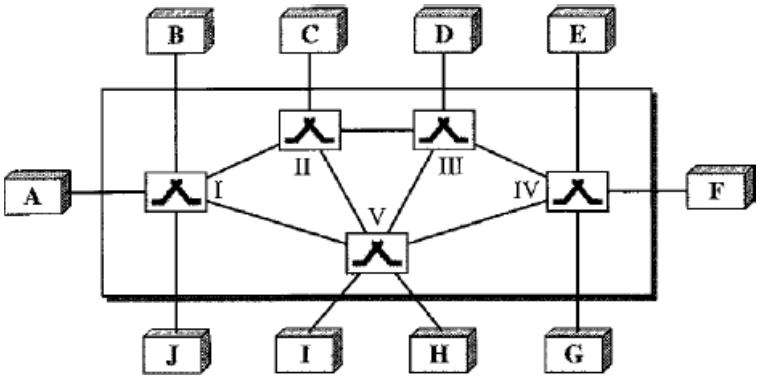
- It requires both transmitter and receiver to be in line of sight.
- Devices cannot move around while transmission is in progress.
- Used for very short distance applications.

1.11 SWITCHING

A network is a set of connected devices. Whenever we have multiple devices, we have the problem of how to connect them to make one-to-one communication possible. One solution is to make a point-to-point connection between each pair of devices (a mesh topology) or between a central device and every other device (a star topology). These methods, however, are impractical and wasteful when applied to very large networks.

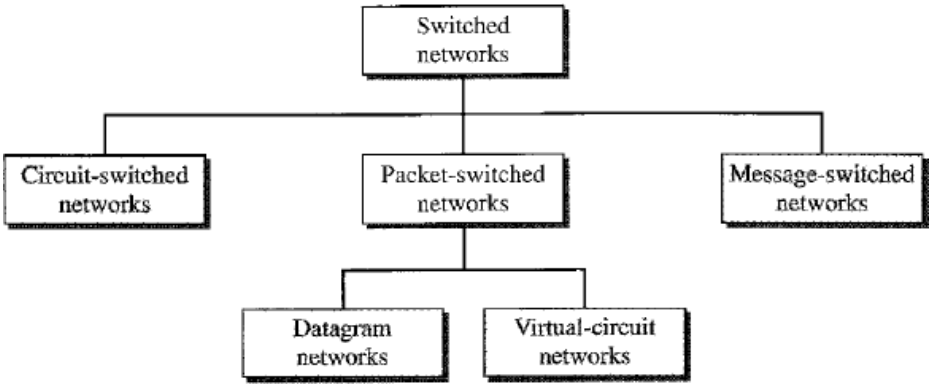
The number and length of the links require too much infrastructure to be cost-efficient, and the majority of those links would be idle most of the time. Other topologies employing multipoint connections, such as a bus, are ruled out because the distances between devices and the total number of devices increase beyond the capacities of the media and equipment.

A better solution is switching. 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. Figure shows a switched network.



The end systems (communicating devices) are labelled A, B, C, D, and so on, and the switches are labelled I, II, III, IV, and V. Each switch is connected to multiple links.

Taxonomy of Switched Networks



1.11.1 Circuit-Switched Networks

A circuit-switched network consists of a set of switches connected by physical links. A connection between two stations is a dedicated path made of one or more links. However, each connection uses only one dedicated channel on each link. Each link is normally divided into n channels by using FDM or TDM

Figure shows a trivial circuit-switched network with four switches and four links. Each link is divided into n (n is 3 in the figure) channels by using FDM or TDM.

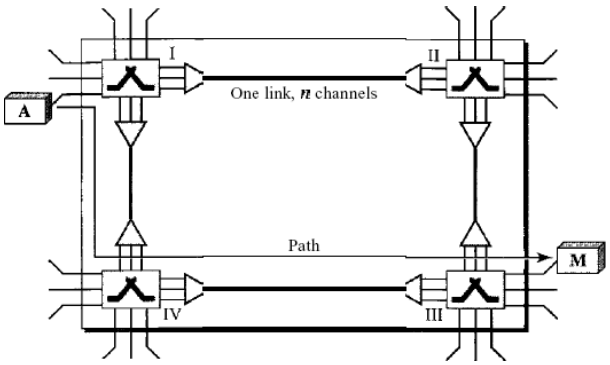


Fig : circuit-switched network

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. Figure above shows the idea of delay in a circuit-switched network when only two switches are involved. As Figure shows, there is no waiting time at each switch. The total delay is due to the time needed to create the connection, transfer data, and disconnect the circuit.

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. Figure 8.6 shows the idea of delay in a circuit-switched network when only two switches are involved. As Figure shows, there is no waiting time at each switch. The total delay is due to the time needed to create the connection, transfer data, and disconnect the circuit.

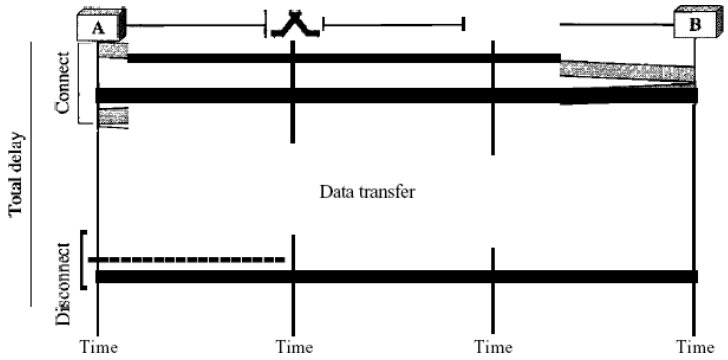


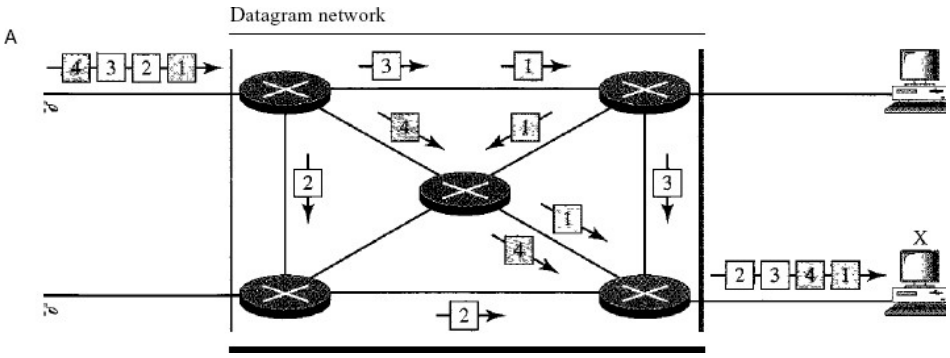
Fig: Delay

The delay caused by the setup is the sum of four parts: the propagation time of the source computer request (slope of the first gray box), the request signal transfer time (height of the first gray box), the propagation time of the acknowledgment from the destination computer (slope of the second gray box), and the signal transfer time of the acknowledgment (height of the second gray box). The delay due to data transfer is the sum of two parts: the propagation time (slope of the colored box) and data transfer time (height of the colored box), which can be very long. The third box shows the time needed to tear down the circuit. We have shown the case in which the receiver requests disconnection, which creates the maximum delay.

7.2 DATAGRAM NETWORKS

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. We briefly discuss datagram networks here as a comparison with circuit-switched and virtual-circuit switched networks Figure shows how the datagram approach is used to deliver four packets from station A to station X. The switches in a datagram network are traditionally referred to as routers. That is why we use a different symbol for the switches in the figure



Packet Switching

In this example, all four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination. This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all the packets from A to X. This approach can cause the datagrams of a transmission to arrive at their destination out of order with different delays between the packets. Packets may also be lost or dropped because of a lack of resources. In most protocols, it is the responsibility of an upper- layer protocol to reorder the datagrams or ask for lost datagrams before passing them on to the application.

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.

Routing Table

If there are no setup or teardown phases, how are the packets routed to their destinations in a datagram network? 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. This is different from the table of a circuit switched network in which each entry is created when the setup phase is completed and deleted when the teardown phase is over. Figure shows the routing table for a switch.

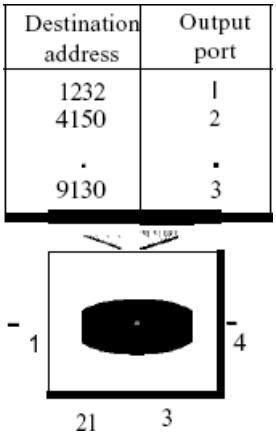


Fig: Routing table in a datagram network

Every packet in a datagram network carries a header that contains, among other information, the destination addresses of the packet. When the switch receives the packet, this destination address is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded. This address, unlike the address in a virtual-circuit-switched network, remains the same during the entire journey of the packet.

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. If a source sends a packet and there is a delay of a few minutes before another packet can be sent, the resources can be reallocated during these minutes for other packets from other sources.

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. In addition, since not all packets in a message necessarily travel through the same switches, the delay is not uniform for the packets of a message

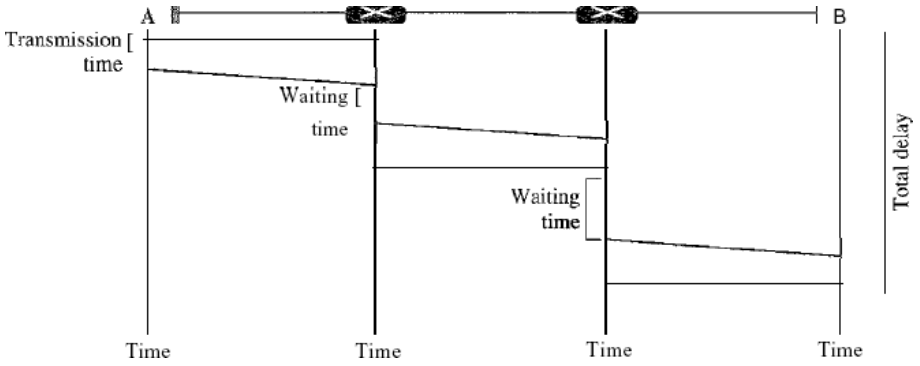


Fig : Delay in a datagram network

The packet travels through two switches. There are three transmission times (3T), three propagation delays (slopes 3't of the lines), and two waiting times (WI + w2)' We ignore the processing time in each switch. The total delay is

Total delay =3T + 3t + WI + W2

Virtual-Circuit Networks:

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

(2) As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.

(3) Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.

(4) As in a datagram network, data are packetized and each packet carries an address in the header. However, the address in the header has local jurisdiction (it defines what should be the next switch and the channel on which the packet is being canied), not end-to-end jurisdiction. The reader may ask how the intermediate switches know where to send the packet if there is no final destination address carried by a packet. The answer will be clear when we discuss virtual- circuit identifiers in the next section.

(5) As in a circuit-switched network, all packets follow the same path established during the connection.

(6) A virtual-circuit network is normally implemented in the data link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer. But this may change in the future. Figure is an example of a virtual-circuit network. The network has switches that allow traffic from sources to destinations. A source or destination can be a computer, packet switch, bridge, or any other device that connects other networks.

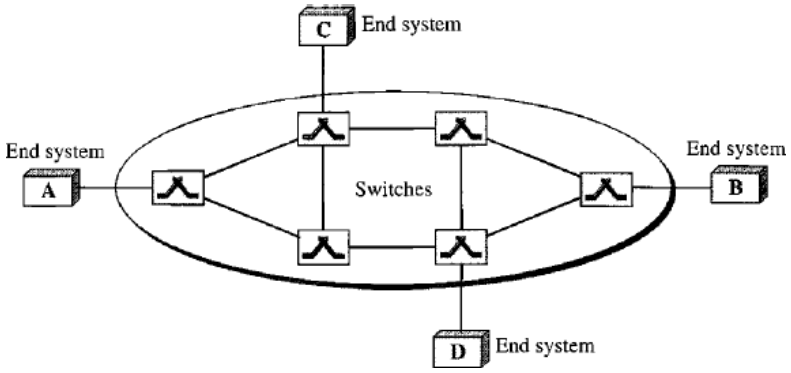


Fig : Virtual-circuit network

Addressing

Fig a: Virtual-circuit network

In a virtual-circuit network, two types of addressing are involved: global and local (virtual-circuit identifier).

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 if the network is part of an international network. However, we will see that a global address in virtual-circuit networks is used only to create a virtual-circuit identifier, as discussed next.

Virtual-Circuit Identifier: The identifier that is actually used for data transfer is called the virtual-circuit identifier (Vel). A vel, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCl. Figure 8.11 shows how the VCI in a data frame changes from one switch to another. Note that a VCI does not need to be a large number since each switch can use its own unique set of VCls

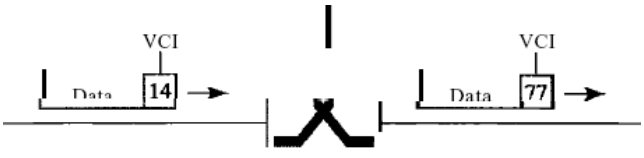


Fig : Virtual-Circuit Identifier

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. We first discuss the data transfer phase, which is more straightforward; we then talk about the setup and teardown phases.

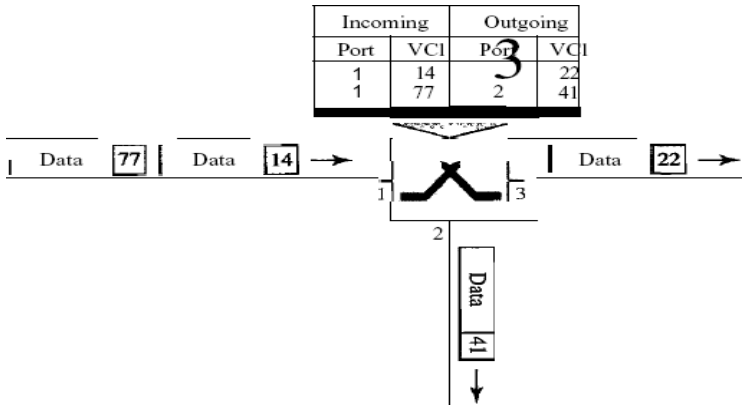
Data Transfer Phase

To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit. The table, in its simplest form, has four columns. This means that the switch holds four pieces of information for each virtual circuit that is already set up. We show later how the switches make their table entries, but for the moment we assume that each switch has a table with entries for all active virtual circuits. Figure 2 shows such a switch and its corresponding table.

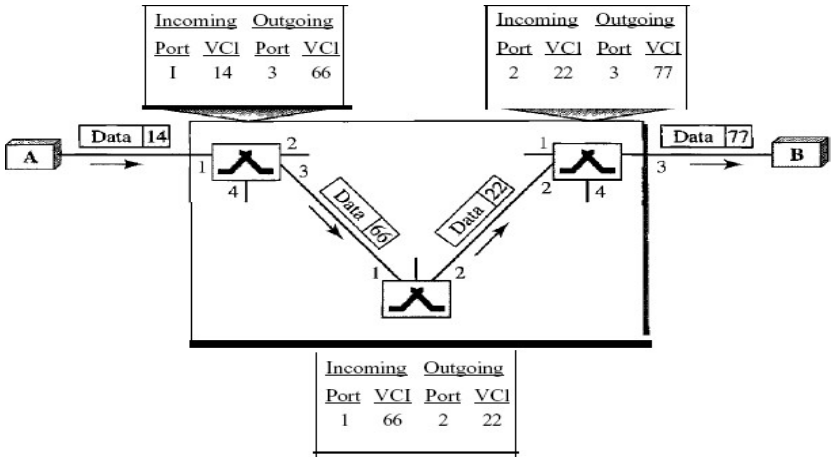
And also shows a frame arriving at port 1 with a VCI of 14. When the frame arrives, the switch looks in its table to find port 1 and a VCI of 14. When it is found, the switch knows to change the VCI to 22 and send out the frame from port 3. Figure 3 shows how a frame from source A reaches destination B and how its VCI changes during the trip. Each switch changes the VCI and routes the frame. The data transfer phase is active until the source sends all its frames to the destination. The procedure at the switch is the same for each frame of a message. The process creates a virtual circuit, not a real circuit, between the source and destination.

Setup Phase

In the setup phase, a switch creates an entry for a virtual circuit. For example, suppose source A needs to create a virtual circuit to B. Two steps are required: the setup request and the acknowledgment.



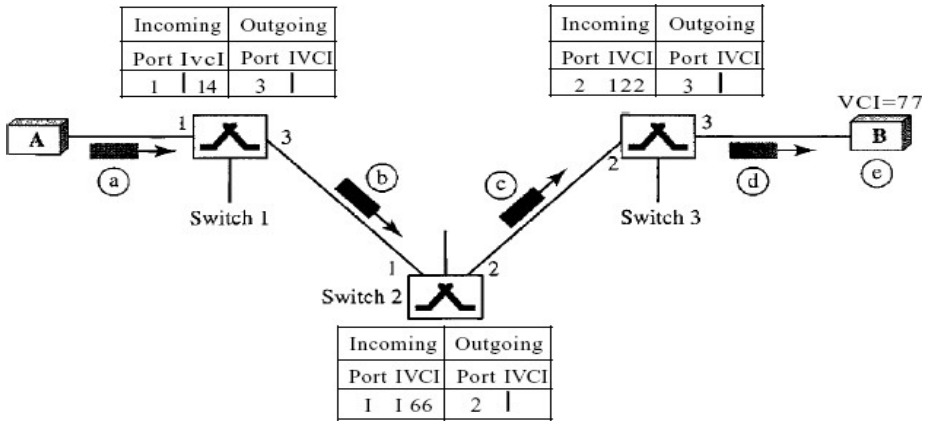
Switch and tables in a virtual-circuit network



Source-to-destination data transfer in a virtual-circuit network

Setup Request

A setup request frame is sent from the source to the destination. Figure 4 shows the process



(a) Source A sends a setup frame to switch 1.

(b) Switch 1 receives the setup request frame. It knows that a frame going from A to B goes out through port 3. How the switch has obtained this information is a point covered in future chapters. The switch, in the setup phase, acts as a packet switch; it has a routing table which is different from the switching table. For the moment, assume that it knows the output port. The switch creates an entry in its table for this virtual circuit, but it is only able to fill three of the four columns. The switch assigns the incoming port (1) and chooses an available incoming VCI (14) and the outgoing port (3). It does not yet know the outgoing VCI, which will be found during the acknowledgment step. The switch then forwards the frame through port 3 to switch 2.

(c) Switch 2 receives the setup request frame. The same events happen here as at switch 1; three columns of the table are completed: in this case, incoming port (l), incoming VCI (66), and outgoing port (2).

(d) Switch 3 receives the setup request frame. Again, three columns are completed: incoming port (2), incoming VCI (22), and outgoing port (3).

(e) Destination B receives the setup frame, and if it is ready to receive frames from A, it assigns a VCI to the incoming frames that come from A, in this case 77. This VCI lets the destination know that the frames come from A, and not other sources.

Acknowledgment A special frame, called the acknowledgment frame, completes the entries in the switching tables. Figure 8.15 shows the process.

(a) The destination sends an acknowledgment to switch 3. The acknowledgment carries the global source and destination addresses so the switch knows which entry in the table is to be completed. The frame also carries VCI 77, chosen by the destination as the incoming VCI for frames from

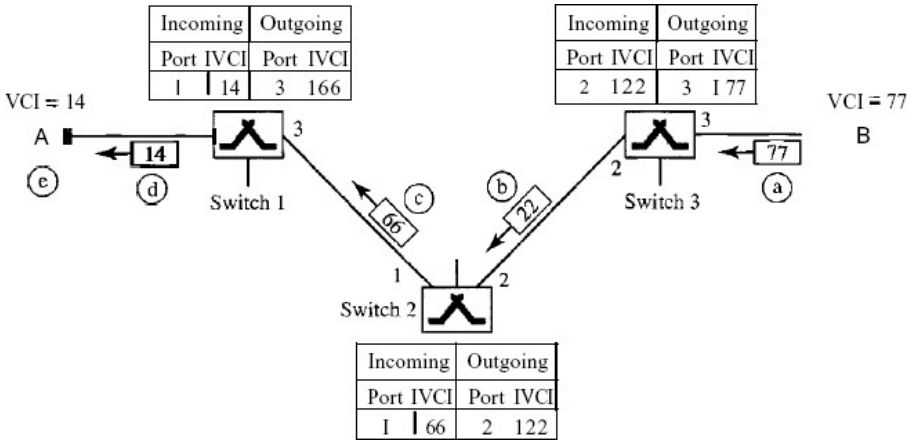
(b) Switch 3 uses this VCI to complete the outgoing VCI column for this entry. Note that 77 is the incoming VCI for destination B, but the outgoing VCI for switch 3.

(c) Switch 3 sends an acknowledgment to switch 2 that contains its incoming VCI in the table, chosen in the previous step. Switch 2 uses this as the outgoing VCI in the table.

(d) Switch 2 sends an acknowledgment to switch 1 that contains its incoming VCI in the table, chosen in the previous step. Switch 1 uses this as the outgoing VCI in the table.

(e) Finally switch 1 sends an acknowledgment to source A that contains its incoming VCI in the table, chosen in the previous step.

(f) The source uses this as the outgoing VCI for the data frames to be sent to destination B.



Setup acknowledgments in a virtual-circuit network

Teardown Phase

In this phase, source A, after sending all frames to B, sends a special frame called a teardown request. Destination B responds with a teardown confirmation frame. All switches delete the corresponding entry from their tables.

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. There is one big advantage in a virtual-circuit network even if resource allocation is on demand.

The source can check the availability of the resources, without actually reserving it. Consider a family that wants to dine at a restaurant. Although the restaurant may not accept reservations (allocation of the tables is on demand), the family can call and find out the waiting time. This can save the family time and effort.

Delay in Virtual-Circuit Networks

In a virtual-circuit network, there is a one-time delay for setup and a one-time delay for teardown. If resources are allocated during the setup phase, there is no wait time for individual packets. Below Figure shows the delay for a packet traveling through two switches in a virtual-circuit network.

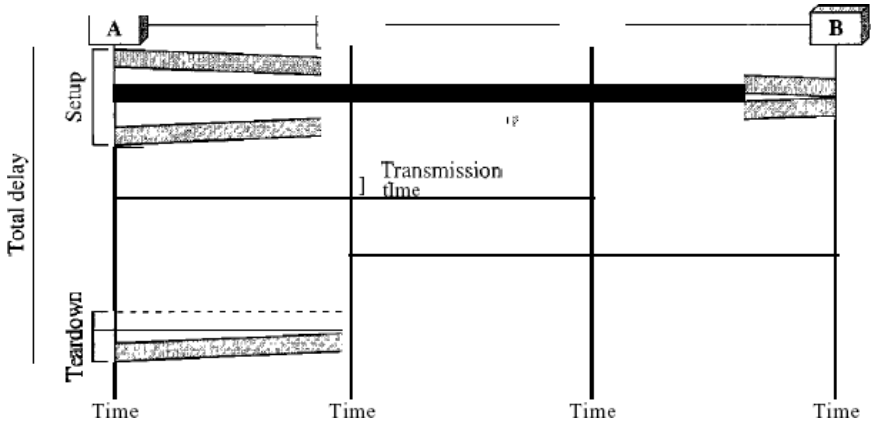


Fig: Delay in a virtual-circuit network

The packet is traveling through two switches (routers). There are three transmission times (3T), three propagation times (3't), data transfer depicted by the sloping lines, a setup delay (which includes transmission and propagation in two directions), and a teardown delay (which includes transmission and propagation in one direction). We ignore the processing time in each switch. The total delay time is

Total delay = 3T+ 3't + setup delay + teardown delay

REVIEW QUESTIONS

PART – A

1) Define networks.

- A network is a set of devices or 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.
- A link can be a cable, air, optical fibber

2) Define computer network.

- A computer network is defined as the interconnection of two or more computers.
- It is done to enable the computers to communicate and share available resources.

3) What are the three criteria necessary for an effective and efficient network?

A network must meet a certain number of criteria to become useable in realworld situation.

Most important of these criteria are the three criteria as follows.

- Performance.
- Reliability.
- Security.

4) List the Application of network.

- Sharing of resources such as printers.
- Sharing of expensive software's and database.
- Communication from one computer to another computer.
- Exchange of data and information among users via network.

5) What are the components of network?

- **Message.** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
- **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.
- **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
- **Protocol**. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.

6) Why protocols are needed on computer network?

- Network protocols are sets of rules for exchanging information.
- This exchange usually occurs much like a dialog between two computers.
- The exchange often begins with the client sending a signal to the server,
- Providing key information about what kind of data is being requested.

7) What are the Functions of OSI layers?

- It describes how applications can communicate over a network.
- It involved when a message is sent from one computer to other computer.
- Each layer should perform a well-defined function.
- The function of each layer should be chosen with stare at toward defining internationally standardized protocols.

8) What are the responsibilities of data link layer?

The data link layer is also responsible for logical link control, media access control, hardware addressing, error detection and handling and defining physical layer standards. It provides reliable data transfer by transmitting packets with the necessary synchronization, error control and flow control. .

9) List the service provides by application layer.

- Network virtual terminal
- File transfer, access, and management
- Mail service
- Directory service.

10) What is the difference between internetworking protocol and internet protocol?

- Internetwork protocol, generally known as network protocol, can be defined as the generic term for the protocols used in computer networks, which include protocols like HTTP, TCP, IP, etc.
- Internet Protocol (IP) is essentially the routed protocol.
- IP operates at the internet layer of the TCP/IP protocol stack (Layer3, network layer in OSI) dealing with IP addressing, to ensure end to delivery.

11) What is the difference between port address, logical address and physical address?

- A logical address is an address similar but it's like the information you would use to get to a physical address.
- A physical address is like your hard drive to your computer.
- A logical address is like a file on the server, with information or instructions that lead to it.

- A port is identified for each address and protocol by a 16-bit number, commonly known as the port number. Specific port numbers are often used to identify specific services.

12) What is the difference between TPC and UDP?

- TCP/IP is a suite of protocols used by devices to communicate over the Internet and most local networks.
- It is named after two of it's original protocols—the Transmission Control Protocol (TCP) and the Internet Protocol (IP).
- TCP provides apps a way to deliver (and receive) an ordered and error-checkedstream of information packets over the network.
- The User Datagram Protocol (UDP) is used by apps to deliver a faster stream ofinformation by doing away with error-checking.

13) What are the features provided by layering?

- It decomposes the problem of building a network into more manageable components.
- It provides a more modular design.

14) Why are protocols needed?

- In networks, communication occurs between the entities in different systems.
- Two entities cannot just send bit streams to each other and expect to be understood.
- For communication, the entities must agree on a protocol.
- A protocol is a set of rules that govern data communication.

15) What are the two interfaces provided by protocols?

- Service interface
- Peer interface
- Service interface- defines the operations that local objects can perform on the protocol.
- Peer interface- defines the form and meaning of messages exchanged between protocol peers to implement the communication service.

16) What are the protocols used in application layer TCP/IP reference model?

- TELNET
- FTP(File Transfer Protocol)
- SMTP(Simple Mail Transport Protocol)
- DNS(Domain Name Server)
- HTTP (Hypertext Transfer Protocol)

17) What is TCP/IP reference model?

- TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well.
- Protocols are set of rules which govern every possible communication over a network.
- These protocols describe the movement of data between the source and destination or the internet. These protocols offer simple naming and addressing schemes.

18) Define layer?

The layer immediately above the hardware in this case might provide host-to-host connectivity, abstracting away the fact that there may be an arbitrarily complex network topology between any two hosts.

19) Define Network topology with their types.

- Network topology is structure of a network and arrangement of the various elements (links, nodes, etc.) of a communication in the network.
- Physical topology is the placement of the various components of a network, including device location and cable installation,
- Logical topology illustrates how data flows within a network.
- Types of Network Topology
- Network topologies are categorized into the following basic types:
  - Bus, Ring, Star, Mesh, Tree and Hybrid

20) What are Common categories of the networks?

- LAN - Local Area Network
- WAN - Wide Area Network
- MAN - Metropolitan Area Network
- WLAN - Wireless Local Area Network

PART – B

(1) Illustrate the basic concepts of computer networks.

(2) Explain the topologies of the networks in detail with diagram.

(3) Explain the categories of the networks in detail with diagram.

(4) Explain in details reference and basic concepts of OSI model.

(5) Describe in details about layer in OSI model.

(6) Explain in details about TCP / IP model.

(7) Explain in details comparison between OSI and TCP/IP model.