Data Communication & Network Standards

Part-3

9.2 TRANSMISSION MODES

- Data is transmitted between two digital devices on the network in the form of bits.
- Transmission mode refers to the mode used for transmitting the data. The transmission medium may be capable of sending only a single bit in unit time or multiple bits in unit time.
- When a single bit is transmitted in unit time the transmission mode used is Serial Transmission and when multiple bits are sent in unit time the transmission mode used is called Parallel transmission.

Types of Transmission Modes:

- There are two basic types of transmission modes Serial and Parallel as shown in the figure below.
- Serial transmission is further categorized into Synchronous and Asynchronous Serial transmission.

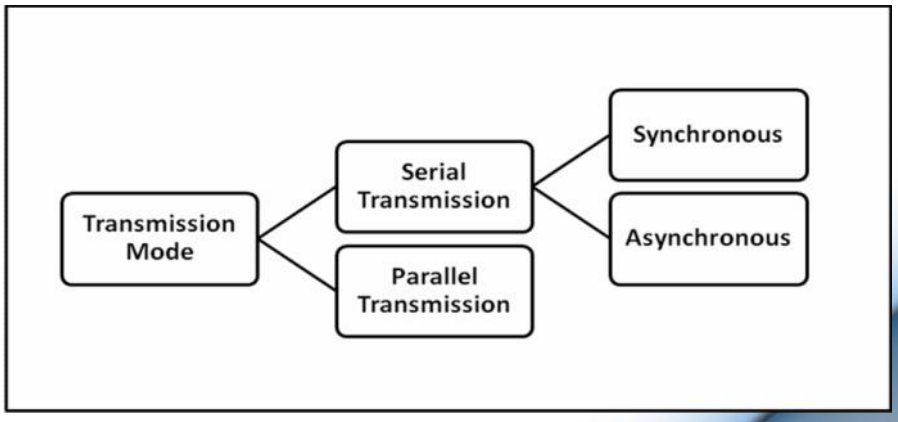


Fig. Types of Transmission Modes

9.2.1 Parallel Transmission

- It involves simultaneous transmission of *N* bits over *N* different channels
- Parallel Transmission increases transmission speed by a factor of *N* over serial transmission
- Disadvantage of parallel transmission is the cost involved, N channels have to be used, hence, it can be used for short distance communication only

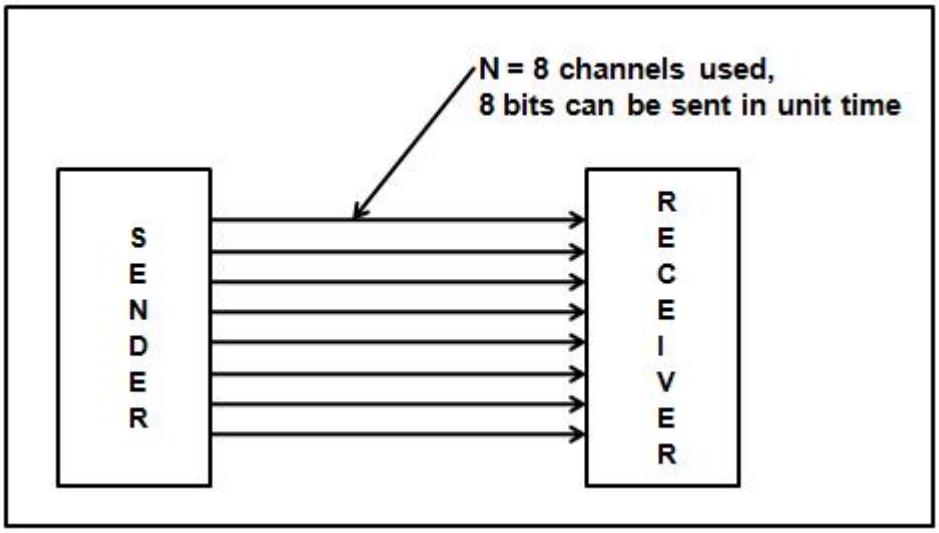


Fig. Parallel Transmission of Data over N = 8 channels

- Example of Parallel Transmission is the communication between CPU and the Projector.

9.2.2 Serial Transmission

- In Serial Transmission, as the name suggests data is transmitted serially, i.e. bit by bit, one bit at a time.
- Since only one bit has to be sent in unit time only a single channel is required.

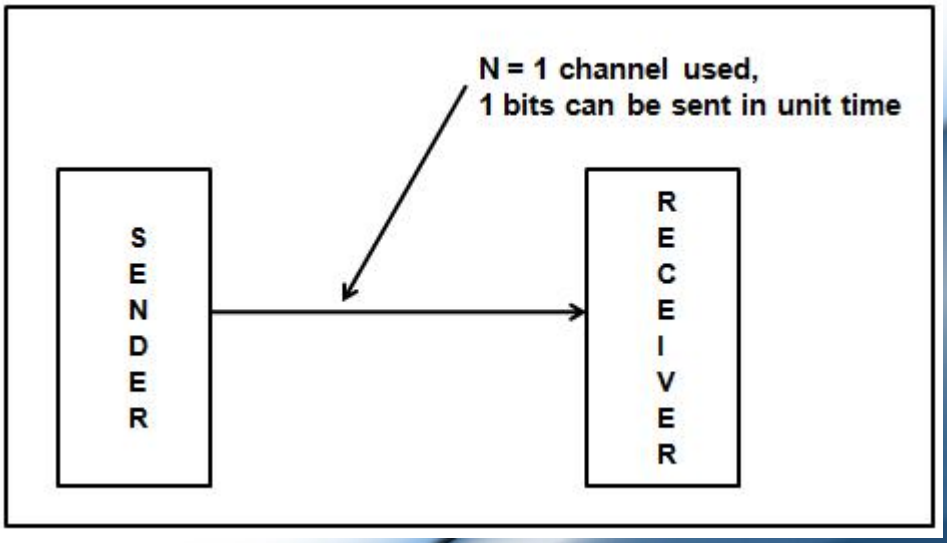


Fig. Serial Transmission of Data over N = 8 channels

Types of Serial Transmission:

Depending upon the timing of transmission of data there are two types of serial transmission as described below

9.2.2.1 ASynchronous Transmission

- In asynchronous serial transmission the sender and receiver are not synchronized.
- The data is sent in group of 8 bits i.e. in bytes.
- The sender can start data transmission at any time instant without informing the receiver.
- To avoid confusing the receiver while receiving the data, —startll and —stopll bits are inserted before and after every group of 8 bits as shown below

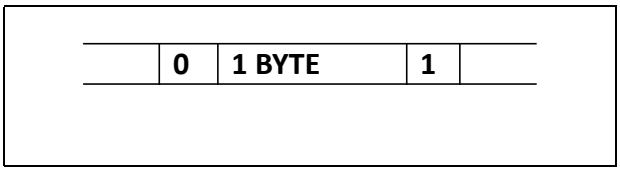


Fig: Start and Bit before and after every data byte

- The start bit is indicated by —0ll and stop bit is indicated by —1ll.
- The sender and receiver may not be synchronized as seen above but at the bit level they have to be synchronized i.e. the duration of one bit needs to be same for both sender and receiver for accurate data transmission.
- There may be gaps in between the data transmission indication that there is no data being transmitted from sender. Ex. Assume a user typing at uneven speeds, at times there is no data being transmitted from Keyboard to the CPU.
- Following is the Diagram for Asynchronous Serial Transmission.

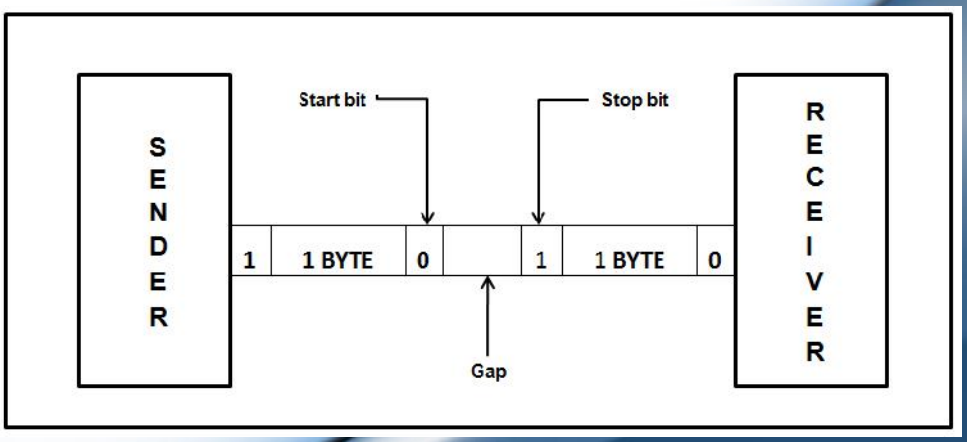


Fig: Asynchronous Serial Transmission

- **Advantages**
  1. Cheap and Effective implementation
  2. Can be used for low speed communication

- **Disadvantages**
  Insertion of start bits, stop bits and gaps make asynchronous transmission slow.

- **Application**
  Keyboard

9.2.2.2 Synchronous Transmission

- In Synchronous Serial Transmission, the sender and receiver are highly synchronized.
- No start, stop bits are used.
- Instead a common master clock is used for reference.
- The sender simply send stream of data bits in group of 8 bits to the receiver without any start or stop bit.
- It is the responsibility of the receiver to regroup the bits into units of 8 bits once they are received.
- When no data is being transmitted a sequence of 0‘s and 1‘s indicating IDLE is put on the transmission medium by the sender.

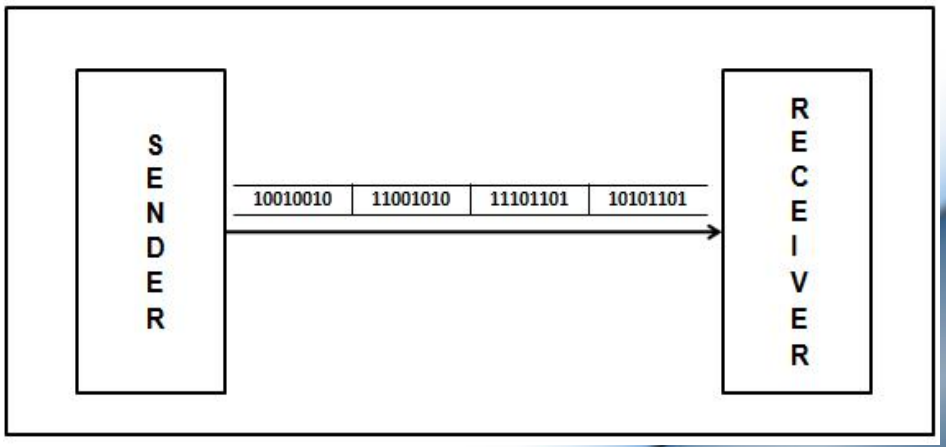


Fig: Asynchronous Serial Transmission

- **Advantage**
  1. There are no start bits, stop bits or gaps between data units
  2. Since the above are absent data transmission is faster.
  3. Due to synchronization there are no timing errors.

9.2.2.3 Comparison of serial and parallel transmission

Sr.no	Parameter	Parallel transmission	Serial transmission
1	Number of wire required to transmit N bits	N wire	1 wire
2	Number of bits transmitted simultaneously	N bits	1 bit
3	Speed of data transfer	False	Slow
4	Cost	Higher due to more number of conductor	Low, since only one wire is used
5	Application	Short distance communication such as computer to printer communication	Long distance computer to computer communication.

9.3 Transmission Impairments & Types

- Data is transmitted through transmission medium which are not perfect.
- The imperfection causes signal impairment.
- Due to the imperfection error is introduced in the transmitted data i.e. the original signal at the beginning of the transmission is not the same as the signal at the Receiver.
- There are three causes of impairment: attenuation, distortion, and noise as shown below:

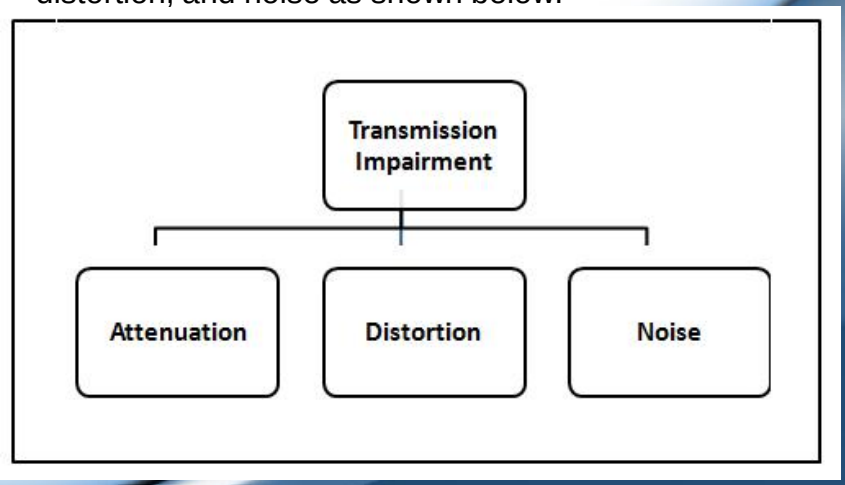


Fig: Transmission Impairment Types

1. Attenuation

- Attenuation results in loss of energy. When a signal travels through a medium, it loses some of its energy in overcoming the resistance of the medium.
- The electrical energy in the signal may converted to heat.
- To compensate for this loss, amplifiers are used to amplify the signal. Figure below shows the effect of attenuation and amplification.

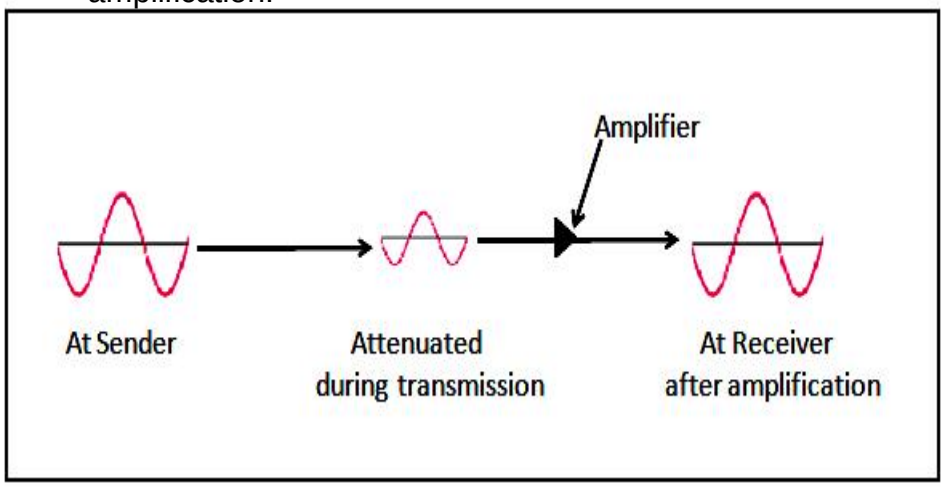


Fig. Attenuation

9.3.2 Distortion

- Distortion changes the shape of the signal as shown below

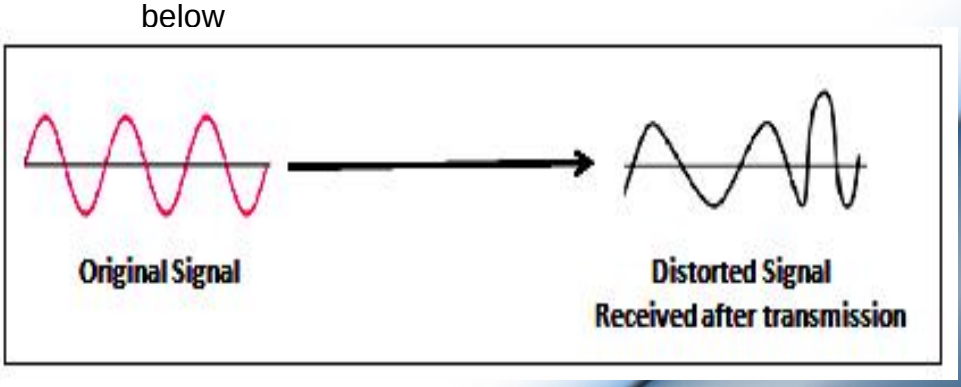


Fig. Distortion

9.3.3 Noise

- Noise is any unwanted signal that is mixed or combined with the original signal during transmission.
- Due to noise the original signal is altered and signal received is not same as the one sent.

4. REVIEW QUESTIONS

1. What is data transmission? What are the different possible ways of transmitting data?
2. Explain Parallel transmission mode
3. Explain Serial transmission mode and list its types
4. Explain Asynchronous serial transmission
5. Explain Synchronous Serial Transmission
6. Write a short note on transmission impairments
7. Differentiate between serial and parallel Transmission

5. REFERENCES & FURTHER READING

Data Communication & Networking – Behrouz Forouzan

10

TRANSMISSION MEDIUM

Unit Structure

1. Objectives
2. Introduction
3. Transmission Medium
    1. Categories of Transmission Medium
4. Guided Transmission Media
    1. Twisted Pair Cable
        10.3.1.1 Unshielded & Shielded Twisted Pair Cable
    2. Co-axial Cable
    3. Fiber Optic Cable
1. Unguided (wireless) Transmission Medium
    1. Propagation Method of wireless signals
    2. Types of wireless transmission
        1. Radio waves
        2. Microwaves
        3. Infrared
5. Comparison between wired and wireless media
6. Comparison between twisted pair cable, co-axial cable and optical fiber
7. Review Questions
8. References & Further Reading

1. OBJECTIVES

In this chapter, you will understand:

- Definition of Transmission Medium and its types
- Different types of Guided Transmission medium
- Different types of UnGuided Transmission medium
- Different ways in which wireless signals are transmitted

2. INTRODUCTION

In Data Communication networking, it is worth understanding the medium through which data passes and what are the available

mediums and their types. This chapter give a thorough understanding of the different types of transmission medium used for data communication

2. TRANSMISSION MEDIA

- Transmission media is ameans by which a communication signal is carried from one system to another
- A transmission medium can be defined as anything that can carry information from a source to a destination.
- The transmission medium is usually free space, metallic cable or fiber – optic cable.

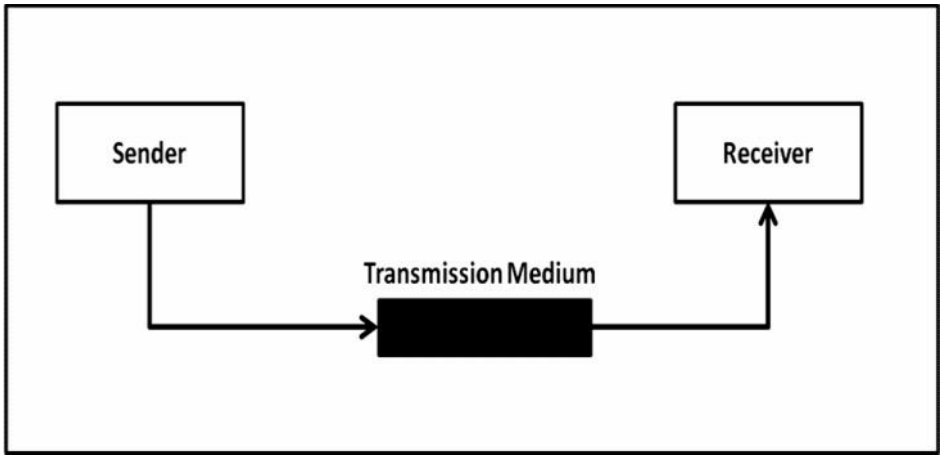


Figure: Transmission of data from sender to receiver through a medium

10.2.1 Categories of transmission media

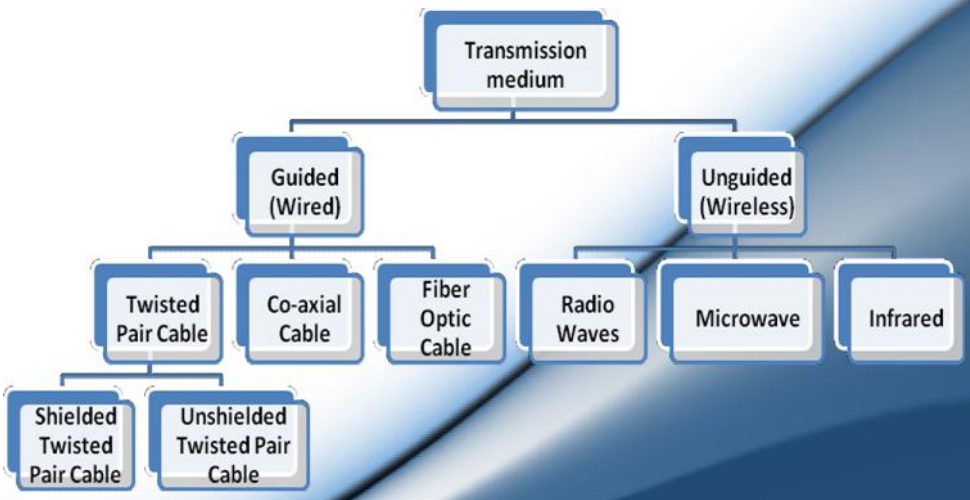


Figure : Categories of Transmission Medium

3. GUIDED MEDIA

- Guided Transmission media uses a cabling system that guides the data signals along a specific path.
- Guided media also known as Bounded media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.
- Out of these twisted-pair cable, coaxial cable transport signals in the form of electric signals and fiber-optic cable transport signals in the form of light.
- Types:
    1. Twisted-Pair Cable
    2. Coaxial Cable
    3. Fiber-OpticCable

10.3.1 Twisted-pair cable

Figure: Twisted Pair Cable

- The wires is twisted twisted together in pairs.
- Each pair would consist of wire used for the +ve data signal and a wire used for the —ve data signal. Any noise that appears on +ve/—ve wire of the pair would occur on the other wire.
- Because the wires are opposite polarities, they are 180 degrees out of phase (180 degree phases or definition of opposite polarity) when the noise appears on both wires, it cancels or nulls itself out at the receiving used.
- Twisted pair cables are most effectively used in a system that uses a balanced line method of transmission.

10.3.1.1 Unshielded Twisted Pair Cable (UTP)& Shielded Twisted Pair Cable (STP)

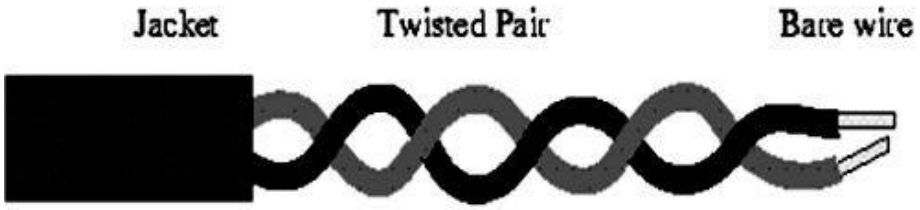


Fig. Unshielded Twisted Pair Cable

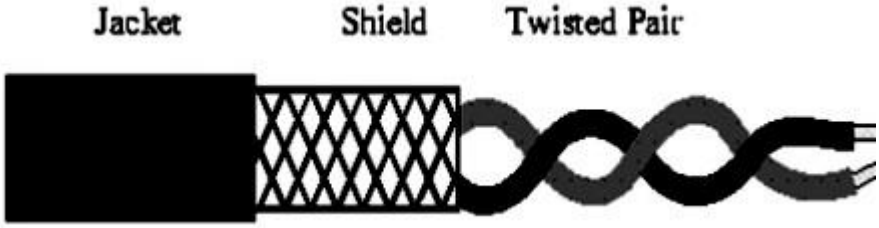


Fig. Shielded Twisted Pair Cable

- Cables with the shield are called shielded twisted pair and commonly abbreviated STP.
- Cables without a shield are called unshielded twisted pair or UTP.
- Twisting the wires together results in characteristics impedance for the cable.
- UTP or unshielded twisted pair cable is used on Ethernet
- UTP cables are used for Ethernet cabling where 4 twisted pair cables (a total of 8 wires are used)

- **10.3.2 Co-Axial Cable**

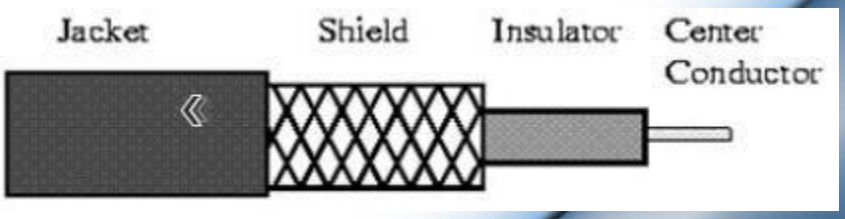


Figure: Co-axial cable

- Coaxial cable consists of 2 conductors.
- The inner conductor is contained inside the insulator with the other conductor weaves around it providing a shield.
- An insulating protective coating called a jacket covers the outer conductor.

- The outer shield protects the inner conductor from outside electrical signals.
- The distance between the outer conductor (Shield) and inner conductor plus the type of material used for insulating the inner conductor determine the cable properties or impedance. The excellent control of the impedance characteristics of the cable allow higher data rates to be transferred than twisted pair cable.

10.3.3 Fibre Optic Cable

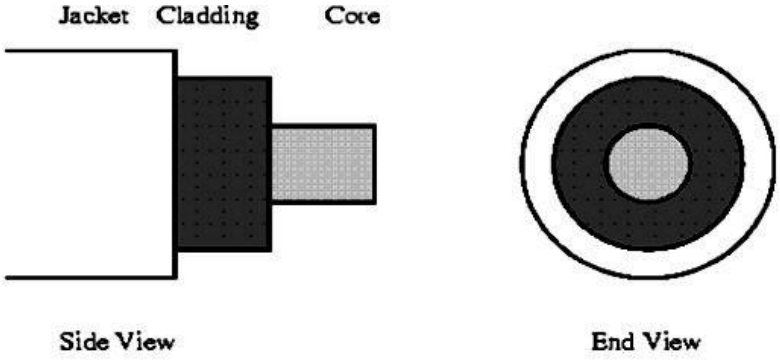


Figure Fiber Optic Cable

- Optical fiber consists of thin glass fiber that can carry information at frequencies in the visible light spectrum.
- The typical optical fiber consists of a very narrow strand of glass called the cladding.
- A typical core diameter is 62.5 microns.
- Typically cladding has a diameter of 125 minors. Coating the cladding is a protective coating consisting of plastic, it is called the jacket.
- The device generating the message has it in electromagnetic form (electrical signal); this has to be converted into light (i.e. optical signal) to send it on optic fiber cable. The process of converting light to electric signal is done on the receiving side.

Advantages:

1. **Small size and light weight**: The size of the optical fibers is very small.Therefore a large number of optical fibers can fit into a cable of small diameter.

2. **Easy availability and low cost**: The material used for the manufacturing of optical fibers is —Silica glass‖. this material is easily available. So the optical fibers cost lower than the cables with metallic conductors.

3. **No electrical or electromagnetic interference:** Since the transmission takes place in the form of light rays the signal is not affected due to any electrical or electromagnetic Interference.

4. **Large Bandwidth**: As the light rays have a very high frequency in GHz range, the bandwidth of the optical fiber is extremely large.

5. **Other advantages**: - No cross talk inside the optical fiber cable. Signal can be sent up to 100 times faster.

10.4 UNGUIDED (WIRELESS) TRANSMISSION MEDIUM

- Unguided media transport data without using a physical conductor. This type of communication is often referred to as wireless communication.

- It uses wireless electromagnetic signals to send data.

- There are three types of Unguided Media
  (i) Radio waves
  (ii) Micro waves
  (iii) Infrared.

- Before understanding the different types of wireless transmission medium, let us first understand the ways in which wireless signals travel. These signals can be sent or propagated in the following three ways:
  1. Ground-wave propagation
  2. Sky-wave propagation
  3. Line-of-sight propagation

1. Ground-wave propagation

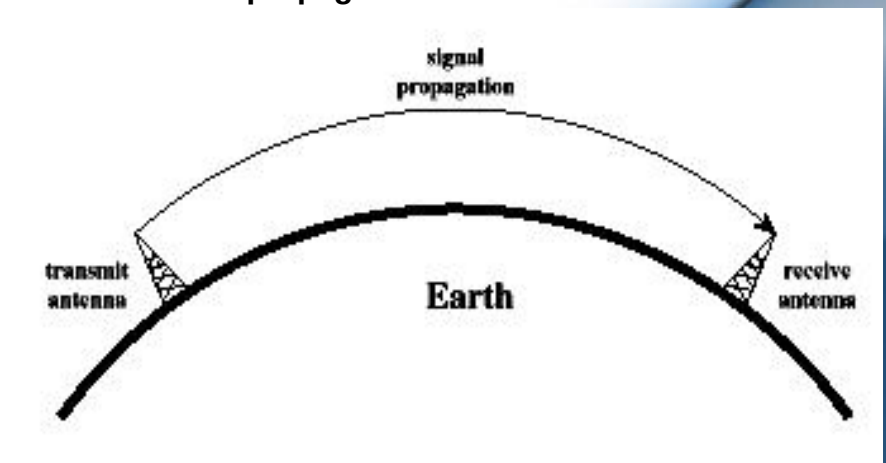


Figure : Ground Propagation of waves

Characteristics of Ground-wave propagation are as follows:

i. Follows contour of the earth
ii. Can Propagate considerable distances
iii. Frequencies up to 2 MHz
iv. Example
    a. AM radio

2. Sky-wave propagation

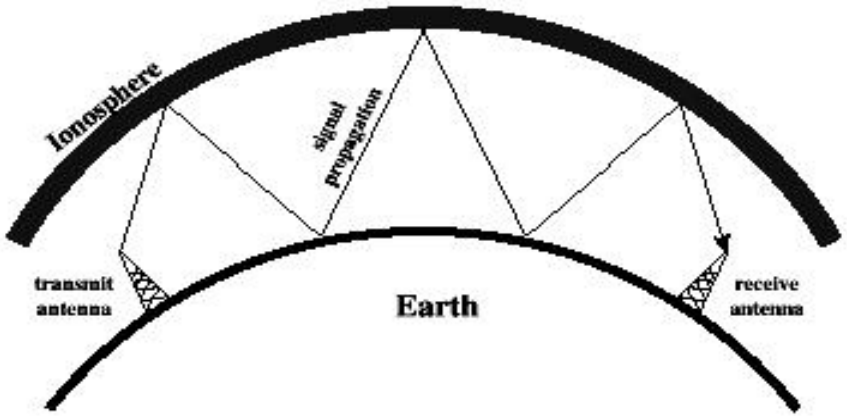


Figure :of waves

Characteristics of Sky Propagation are as follows:

i. Signal reflected from ionized layer of atmosphere back down to earth
ii. Signal can travel a number of hops, back and forth between ionosphere and earth‘s surface
iii. Reflection effect caused by refraction
iv. Examples
    a. Amateur radio
    b. CB radio

3. Line-of-sight propagation

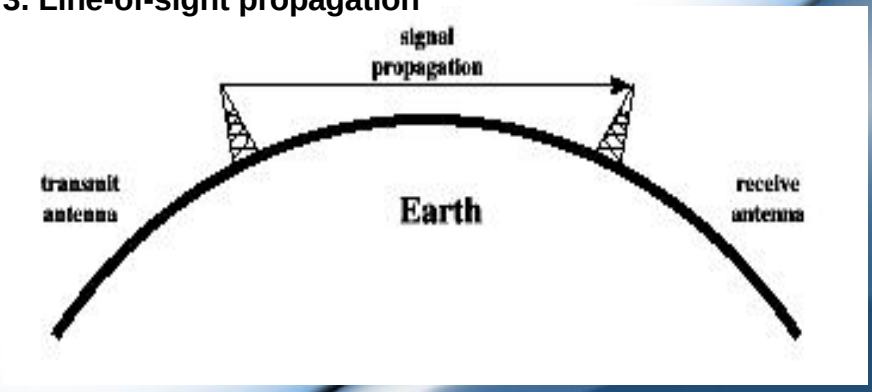


Figure : Line of Sight Propagation of waves

Characteristics of Line of Sight Propagation are as follows:

i. Transmitting and receiving antennas must be within line of sight
    a. Satellite communication – signal above 30 MHz not reflected by ionosphere
    b. Ground communication – antennas within *effective* line of site due to refraction

1. **Radio waves:**

- Electromagnetic wave ranging in frequencies between 3 KHz and 1GHz are normally called radio waves.

- Radio waves are omni-directional when an antenna transmits radio waves they are propagated in all directions. This means that sending and receiving antenna do not have to he aligned. A sending antenna can send waves that can be received by any receiving antenna.

- Radio waves particularly those waves that propagate in sky mode, can travel long distances. This makes radio waves a good candidate for long-distance broadcasting such as AM radio.

- Radio waves particularly those of low and medium frequencies can penetrate walls. It is an advantage because; an AM radio can receive signals inside a building. It is the disadvantage because we cannot isolate a communication to first inside or outside a building.

2. Microwaves:

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

- Microwaves are unidirectional; when an antenna transmits microwaves they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.

- Microwaves propagation is line-of-sight. Since the towers with the mounted antennas needs to be in direct sight of each other, towers that are far apart need to be very tall, the curvature of the earth as well as other blocking obstacles do not allow two short towers to communicate using microwaves, Repeaters are often needed for long distance communication very high frequency microwaves cannot penetrate walls.

- Parabolic dish antenna and horn antenna are used for this means of transmission

3. Infrared

- Infrared signals with frequencies ranges from 300 GHz to 400 GHz can be used for short range communication.

- Infrared signals, having high frequencies, cannot penetrate walls. This helps to prevent interference between one system and another. Infrared Transmissionin one room cannot be affected by the infrared transmission in another room.

- Infrared band, has an excellent potential for data transmission. Transfer digital data is possible with a high speed with a very high frequency. There are number of computer devices which are used to send the data through infrared medium e.g. keyboard mice, PCs and printers. There are some manufacturers provide a special part called the IrDA port that allows a wireless keyboard to communicate with a PC.

10.5 COMPARISON BETWEEN WIRED AND WIRELESS MEDIA

Wired media	Wireless media
The signal energy is contained and guided within a solid medium	The signal energy propagates in the form of unguided electromagnetic waves.
Twisted pair wires, coaxial cable, optical fiber cables are the examples of wired media.	Radio and infrared lights are the examples of wireless media.
Used for point to point communication	Used for radio broadcasting in all direction
Wired media lead to discrete network topology	Wireless media leads to continuous network topology
Additional transmission capacity can be procured by adding more wire	It is not possible procure additional capacity.
Installation is costly and time consuming	Installation needs less time and money
Attenuation depends exponentially on the distance	Attenuation is proportional to square of the distance.

10.6 COMPARISON BETWEEN TWISTED PAIR CABLE, CO-AXIAL CABLE AND OPTICAL FIBER

Twisted pair cable	Co-axial cable	Optical fiber
Transmission of signals take place in the electrical form over the metallic conducting wires.	Transmission of signals take place in the inner conductor of the cable	Signal transmission takes place in an optical form over a glass fiber.
Noise immunity is low. Therefore more distortion	Higher noise immunity than the twisted pair cable due to the presence of shielding conductor	Higher noise immunity as the light rays are unaffected by the electrical noise.
Affected due to external magnetic field	Less affected due to external magnetic field	Not affected by the external magnetic field.
Short circuit between the two conductor is possible	Short circuit between the two conductor is possible	Short circuit is not possible
Cheapest	Moderately expensive	Expensive
Can support low data rates	Moderately high data rate	Very high data rates.
Low bandwidth	Moderately high bandwidth	Very high bandwidth
Easy to installed	Installation is fairly easy	Installation is difficult

10.7 REVIEW QUESTIONS

1. Write short note on transmission medium and explain its different types.
2. Explain Twisted Pair Cables in detail
3. Explain Fiber Optic Cables with its advantages
4. Explain the different ways is which wireless signals propogate.

5. Write short notes on :
   a) Radio waves
   b) Microwaves
   c) Infrared

8. REFERENCES & FURTHER READING

a) Data Communication & Networking – BehrouzForouzan
b) Computer Networks – Andrew Tannenbaum

❖❖❖❖

11

NETWORK TOPOLOGIES

Unit Structure

11.0 OBJECTIVES

- To understand various network strategies and topologies, you will:
- Examine three common strategies used to connect nodes on a network.
- Explore network processing strategies and establish the differences between centralized and distributed processing.
- Identify and compare three common network classifications.
- Identify and define three common network topologies.

11.1 INTRODUCTION

This chapter presents an outline on Network topology is the layout pattern of interconnections of the various elements (links, nodes, etc.) of a computer or biological network. Network topologies may be physical or logical.

Physical topology refers to the physical design of a network including the devices, location and cable installation. Logical topology refers to how data is actually transferred in a network as opposed to its physical design. In general physical topology relates to a core network whereas logical topology relates to basic network. This chapter also presents an insight into the various networking strategies and the platform needed for networking.

11.2 AN OVERVIEW OF NETWORK

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

Two very common types of networks include:

- Local Area Network (LAN)
- Wide Area Network (WAN)

You may also see references to a Metropolitan Area Networks (MAN), a Wireless LAN (WLAN), or a Wireless WAN (WWAN).

11.3 WHAT IS A NETWORK TYPE

1. Local Area Network

A Local Area Network (LAN) is a network that is confined to a relatively small area. It is generally limited to a geographic area such as a writing lab, school, or building.

Computers connected to a network are broadly categorized as servers or workstations. Servers are generally not used by humans directly, but rather run continuously to provide "services" to the other computers (and their human users) on the network. Services provided can include printing and faxing, software hosting, file storage and sharing, messaging, data storage and retrieval, complete access control (security) for the network's resources, and many others.

Workstations are called such because they typically do have a human user which interacts with the network through them. Workstations were traditionally considered a desktop, consisting of a computer, keyboard, display, and mouse, or a laptop, with with integrated keyboard, display, and touchpad. With the advent of the tablet computer, and the touch screen devices such as iPad and iPhone, our definition of workstation is quickly evolving to include those devices, because of their ability to interact with the network and utilize network services.

Servers tend to be more powerful than workstations, although configurations are guided by needs. For example, a group of servers might be located in a secure area, away from humans, and only accessed through the network. In such cases, it would be common for the servers to operate without a dedicated display or keyboard. However, the size and speed of the server's processor(s), hard drive, and main memory might add dramatically to the cost of the system. On the other hand, a workstation might not need as much storage or working memory, but might require an expensive display to accommodate the needs of its user. Every computer on a network should be appropriately configured for its use.

2. Wide Area Network

Wide Area Networks (WANs) connect networks in larger geographic areas, such as Maharashtra, India, or the world. Dedicated transoceanic cabling or satellite uplinks may be used to connect this type of global network.

Using a WAN, schools in Maharashtra can communicate with places like Tokyo in a matter of seconds, without paying enormous phone bills. Two users a half-world apart with workstations equipped with microphones and a webcams might teleconference in real time. A WAN is complicated. It uses multiplexers, bridges, and routers to connect local and metropolitan networks to global communications networks like the Internet. To users, however, a WAN will not appear to be much different than a LAN.

11.4Comparing types of network coverage

The table below compares the three types of networks:

LAN	MAN	WAN
Relatively small.	Can incorporate multiple LANs.	Uses data transmission networks to incorporate LANs and MANs.
Contained within a single building or campus.	Contained within a single city or metropolitan area.	Essentially unlimited geographic area.
Generally inexpensive to implement and maintain.	Expensive to implement and maintain.	Cost varies widely, depending on how it is configured.
Typically owned privately.	Typically owned by private providers.	

11.5 AN ILLUSTRATED EXAMPLE OF A UNIVERSITY NETWORK

Advantages of Installing a Network

- *User access control.*
  Modern networks almost always have one or more servers which allows centralized management for users and for network resources to which they have access. User credentials on a privately-owned and operated network may be as simple as a user name and password, but with ever-increasing attention to computing security issues, these servers are critical to ensuring that sensitive information is only available to authorized users.

- *Information storing and sharing.*
  Computers allow users to create and manipulate information. Information takes on a life of its own on a network. The network provides both a place to store the information and mechanisms to share that information with other network users.

- *Connections.*
  Administrators, instructors, and even students and guests can be connected using the campus network.

- *Services.*
  The institution can provide services, such as registration, college directories, course schedules, access to research, and email accounts, and many others. (Remember, network services are generally provided by servers).

- *Internet.*
  The institution can provide network users with access to the internet, via an internet gateway.

- *Computing resources.*
  The institution can provide access to special purpose computing devices which individual users would not normally own. For example, an institution network might have high-speed high quality printers strategically located around a campus for instructor or student use.

- *Flexible Access.*
  Institution networks allow students to access their information from connected devices throughout the school. Students can begin an assignment in their classroom, save part of it on a public access area of the network, then go to the media center after school to finish their work. Students can also work cooperatively through the network.

- *Workgroup Computing.*

Collaborative software allows many users to work on a document or project concurrently. For example, educators located at various institution within a county could simultaneously contribute their ideas about new curriculum standards to the same document, spreadsheets, or website.

Disadvantages of Installing a Network

- *Expensive to Install.*
  Large campus networks can carry hefty price tags. Cabling, network cards, routers, bridges, firewalls, wireless access points, and software can get expensive, and the installation would certainly require the services of technicians. But, with the ease of setup of home networks, a simple network with internet access can be setup for a small campus in an afternoon.

- *Requires Administrative Time.*
  Proper maintenance of a network requires considerable time and expertise. Many schools have installed a network, only to find that they did not budget for the necessary administrative support.

- *Servers Fail.*
  Although a network server is no more susceptible to failure than any other computer, when the files server "goes down" the entire network may come to a halt. Good network design practices say that critical network services (provided by servers) should be redundant on the network whenever possible.

- *Cables May Break.*
  The Topology chapter presents information about the various configurations of cables. Some of the configurations are designed to minimize the inconvenience of a broken cable; with other configurations, one broken cable can stop the entire network.

- *Security and compliance.*
  Network security is expensive. It is also very important. An institution network would possibly be subject to more

stringent security requirements than a similarly-sized corporate network, because of its likelihood of storing personal and confidential information of network users, the danger of which can be compounded if any network users are minors. A great deal of attention must be paid to network services to ensure all network content is appropriate for the network community it serves.

11.6 WHAT IS A TOPOLOGY?

A *topology* is a description of the layout of a specific region or area. A *network topology* is a description of the layout of the region or area covered by that network.

There are two types of connections that describe how many devices connect to a single cable or segment of transmission media. They are: point-to-point and multi-point.

Point-to-point connections provide a direct link between two devices; for example, a computer connected directly to a printer, or a modem to a mainframe.

Multi-point connections provide a link between three or more devices on a network. All computer networks rely upon point-to-point and multi-point connections.

11.6.1 The Technical Connotation of Topology

The virtual shape or structure of a network is referred as topology.

The pattern or layout of interconnections of different elements or nodes of a computer network is a network topology that might be logical or physical.

However, the complete physical structure of the cable (or transmission media) is called the *physical topology*. The physical topology of a network refers to the configuration of cables, computers, and other peripherals.

The way data flows through the network (or transmission media) is called the *logical topology*. A logical topology is the method used to pass information between workstations.

2. What are the Basic Types of Topology?

There are seven basic topologies in the study of network topology:

1. Point-to-point topology,
2. Bus (point-to-multipoint) topology,
3. Ring topology,
4. Star topology,
5. Hybrid topology,
6. Mesh topology and
7. Tree topology.

The interconnections between computers whether logical or physical are the foundation of this classification.

Logical topology is the way a computer in a given network transmits information, not the way it looks or connected, along with the varying speeds of cables used from one network to another.

On the other hand the **physical topology** is affected by a number of factors:

- Troubleshooting technique,
- Installation cost,
- Office layout and
- Cables‘ types.

The physical topology is figured out on the basis of a network‘s capability to access media and devices, the fault tolerance desired and the cost of telecommunications circuits.

The classification of networks by the virtue of their physical span is as follows: Local Area Networks (LAN), Wide Area Internetworks (WAN) and Metropolitan Area Networks or campus or building internetworks.

11.6.3 How Is the Physical Topology Classified?

- **Point-to-Point Network Topology**

It is the basic model of typical telephony. The simplest topology is a permanent connection between two points. The value

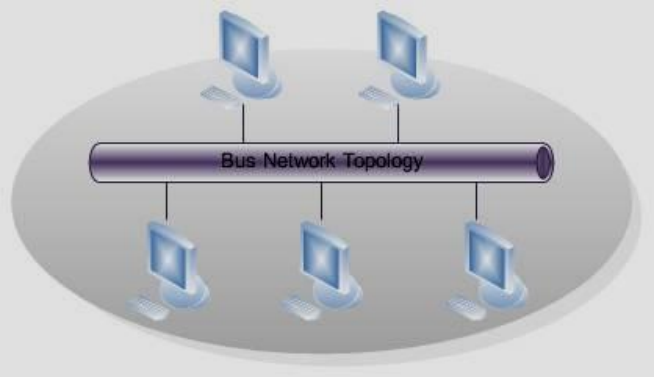
of a demanding point-to-point network is proportionate to the number of subscribers‘ potential pairs. It is possible to establish a permanent circuit within many switched telecommunication systems: the telephone present in a lobby would always connect to the same port, no matter what number is being dialed. A switch connection would save the cost between two points where the resources could be released when no longer required.

- **Bus Network Topology**

LANs that make use of bus topology connects each node to a single cable. Some connector connects each computer or server to the bus cable. For avoiding the bouncing of signal a terminator is used at each end of the bus cable. The source transmits a signal that travels in both directions and passes all machines unless it finds the system with IP address, the intended recipient. The data is ignored in case the address is unmatched. The installation of one cable makes bus topology an inexpensive solution as compared to other topologies; however the maintenance cost is high. If the cable is broken all systems would collapse.

o**Linear Bus:** If all network nodes are connected to a combine transmission medium that has two endpoints the Bus is Linear. The data transmitted between these nodes is transmitted over the combine medium and received by all nodes simultaneously.

o**Distributed Bus:** If all network nodes are connected to a combine transmission medium that has more than two endpoints created by branching the main section of the transmitting medium.



A linear bus topology consists of a main run of cable with a terminator at each end (See fig. 1). All nodes (file server, workstations, and peripherals) are connected to the linear cable. *A bus topology* uses one long cable (backbone) to which network

devices are either directly attached or are attached by using short drop cables. Because all workstations share this bus, a workstation checks for any information that might be coming down the backbone before sending their messages. All messages pass the other workstations on the way to their destinations. Each workstation then checks the address of each message to see if it matches its own. Note that bus network topologies, the backbone must be terminated at both ends to remove the signal from the wire after it has passed all devices on the network.

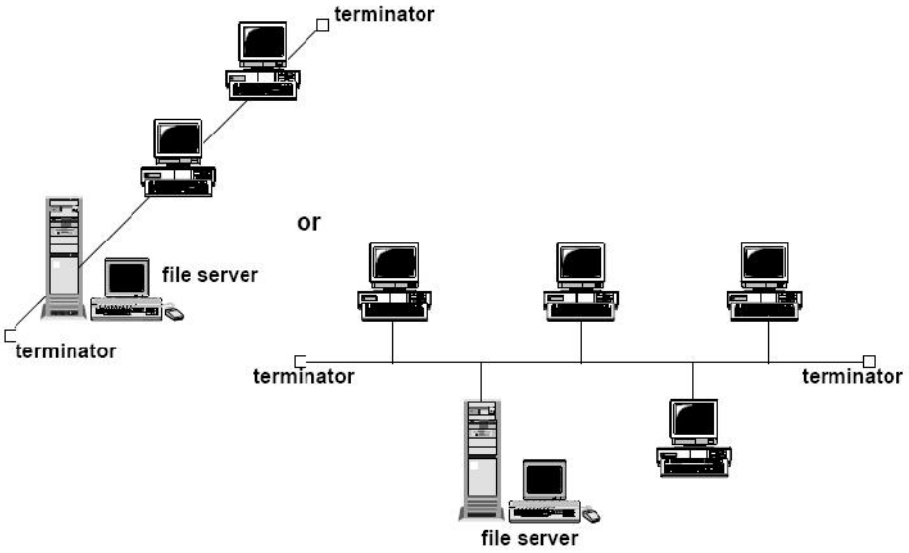


Fig. 1. Linear Bus topology

Advantages of a Linear Bus Topology

- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.

Disadvantages of a Linear Bus Topology

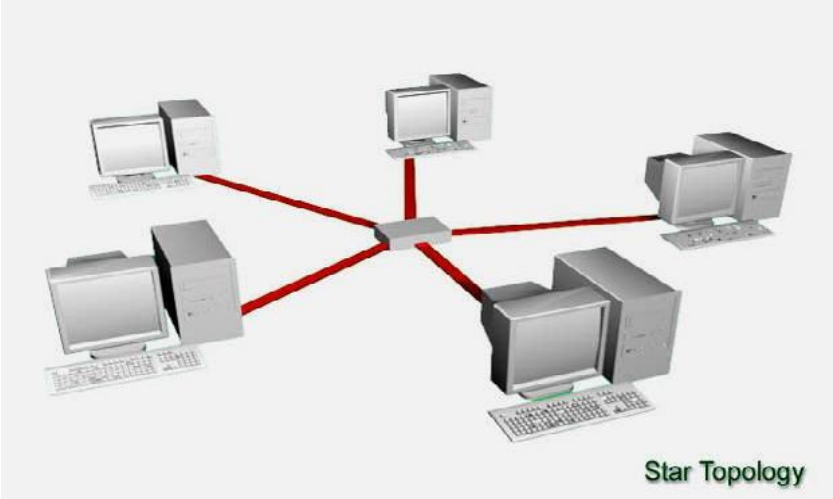
- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.
- Not meant to be used as a stand-alone solution in a large building.

- **Star Network Topology**

The topology when each network host is connected to a central hub in LAN is called Star. Each node is connected to the hub with a point-to-point connection. All traffic passes through the hub that serves as a repeater or signal booster. The easiest topology to install is hailed for its simplicity to add more nodes but criticized for making hub the single point of failure. The network could be BMA (broadcast multi-access) or NBMA (non-broadcast multi-access) depending on whether the signal is automatically propagated at the hub to all spokes or individually spokes with those who are addressed.

o **Extended Star:** A network that keeps one or more than one repeaters between the central node or hub and the peripheral or the spoke node, supported by the transmitter power of the hub and beyond that supported by the standard of the physical layer of the network.

o **Distributed Star:** The topology is based on the linear connectivity that is Daisy Chained with no top or centre level connection points.



Advantages of a Star Topology

- Easy to install and wire.
- No disruptions to the network when connecting or removing devices.
- Easy to detect faults and to remove parts.

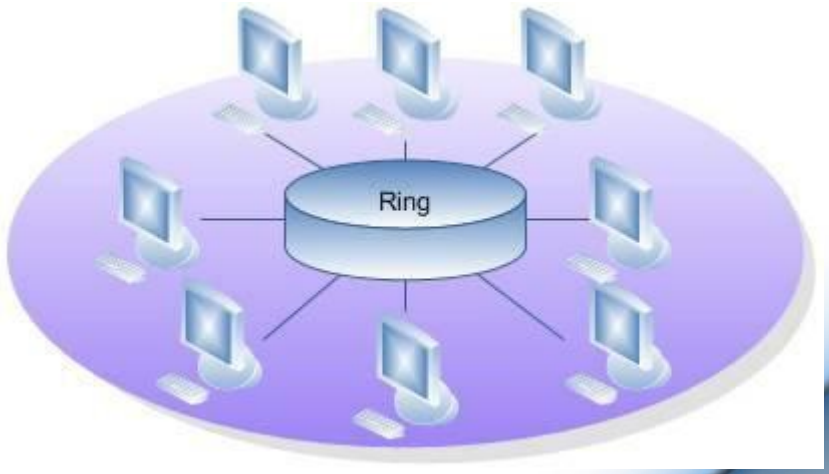
Disadvantages of a Star Topology

- Requires more cable length than a linear topology.
- If the hub, switch, or concentrator fails, nodes attached are disabled.
- More expensive than linear bus topologies because of the cost of the hubs, etc.

Ring Network Topology

Ring topology is one of the old ways of building computer network design and it is pretty much obsolete. FDDI, SONET or Token Ring technologies are used to build ring technology. It is not widely popular in terms of usability but incase if you find it anywhere it will mostly be in schools or office buildings.

Such physical setting sets up nodes in a circular manner where the data could travel in one direction where each device on the right serves as a repeater to strengthen the signal as it moves ahead.

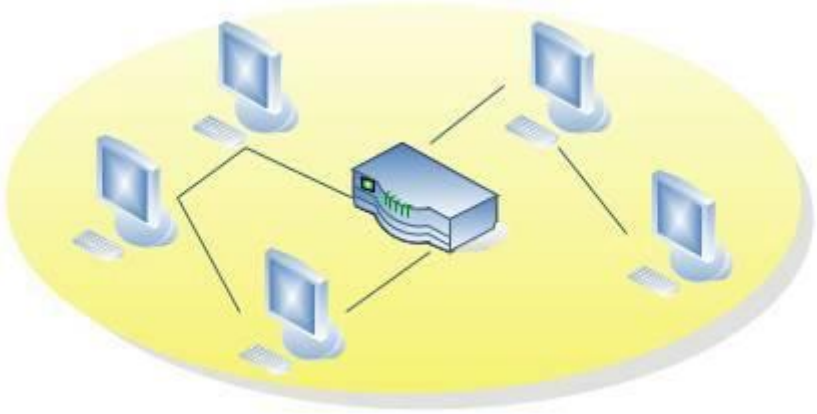


- **Mesh Network Topology**

The exponent of the number of subscribers is proportionate to the value of the fully meshed networks.

o **Fully Connected:** For practical networks such topology is too complex and costly but highly recommended for small number of interconnected nodes.

- **Partially Connected:** This set up involves the connection of some nodes to more than one nodes in the network via point-to-point link. In such connection it is possible to take advantage of the redundancy without any complexity or expense of establishing a connection between each node.

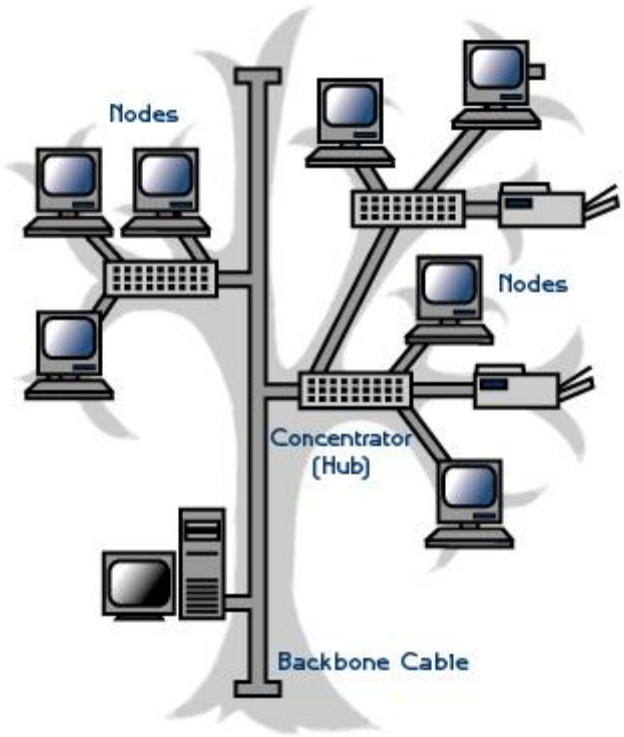


- **Hybrid Topology**

  Hybrid topologies are a combination of two or more different topologies. WANs sometimes have hybrid topologies because they connect a variety of LAN topologies. The big advantage of hybrid topologies is that they connect disparate topologies. However, the disadvantage of hybrid topologies is that they are potentially complex to establish and manage.

- **Tree Network Topology**

The top level of the hierarchy, the central root node is connected to some nodes that are a level low in the hierarchy by a point-to-point link where the second level nodes that are already connected to central root would be connected to the nodes in the third level by a point-to-point link. The central root would be the only node having no higher node in the hierarchy. The tree hierarchy is symmetrical. The BRANCHING FACTOR is the fixed number of nodes connected to the next level in the hierarchy. Such network must have at least three levels. Physical Linear Tree Topology would be of a network whose Branching Factor is one.



Advantages of a Tree Topology

- Point-to-point wiring for individual segments.
- Supported by several hardware and software venders.

Disadvantages of a Tree Topology

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.

Considerations When Choosing a Topology

- **Money**. A linear bus network may be the least expensive way to install a network; you do not have to purchase concentrators.

- **Length of cable needed**. The linear bus network uses shorter lengths of cable.

- **Future growth**. With a star topology, expanding a network is easily done by adding another concentrator.

- C**able type**. The most common cable in schools is unshielded twisted pair,

11.7 SUMMARY

- Knowledge of networking topologies is of core importance of computer networking design. Computer networks can only be developed using the knowledge about these topologies and decide to which topology design is best suited according to the requirement.

- A computer **network** consists of **nodes** and communication **links** whichimplement its **protocols**. It interconnects a set of **hosts** which conform to thenetwork protocols.

- A network may be classified as a **LAN**, **MAN**, or **WAN**, depending on itsgeographic spread, and as **private** or **public**, depending on its accessrestrictions.

- It may employ a **point-to-point** or a **broadcast** communication model. A point-to-point model may be based on **circuit switching** or **packetswitching**.

12

INTRODUCTION TO ROUTING

Unit Structure

12.0 OBJECTIVE

- Introduction to switches and router
- Routing concept
- Concept of switching
- Routing algorithms
- Static and dynamic routing
- Routing metrics

12.0 WHAT IS ROUTING?

Routing is the act of moving information across an internetwork from a source to a destination. Along the way, at least one intermediate node typically is encountered. Routing is often contrasted with bridging, which might seem to accomplish precisely the same thing to the casual observer. The primary difference between the two is that bridging occurs at Layer 2 (the link layer) of the OSI reference model, whereas routing occurs at Layer 3 (the network layer). This distinction provides routing and bridging with different information to use in the process of moving information from source to destination, so the two functions accomplish their tasks in different ways.

1. Routing Components

Routing involves two basic activities: determining optimal routing paths and transporting information groups (typically called packets) through an internetwork. In the context of the routing process, the latter of these is referred to as packet switching. Although packet switching is relatively straightforward, path determination can be very complex.

2. Path Determination

Routing protocols use metrics to evaluate what path will be the best for a packet to travel. A metric is a standard of measurement, such as path bandwidth, that is used by routing algorithms to determine the optimal path to a destination. To aid the process of path determination, routing algorithms initialize and maintain routing tables, which contain route information. Route information varies depending on the routing algorithm used.

Routing algorithms fill routing tables with a variety of information. Destination/next hop associations tell a router that a particular destination can be reached optimally by sending the packet to a particular router representing the —next hopll on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop.

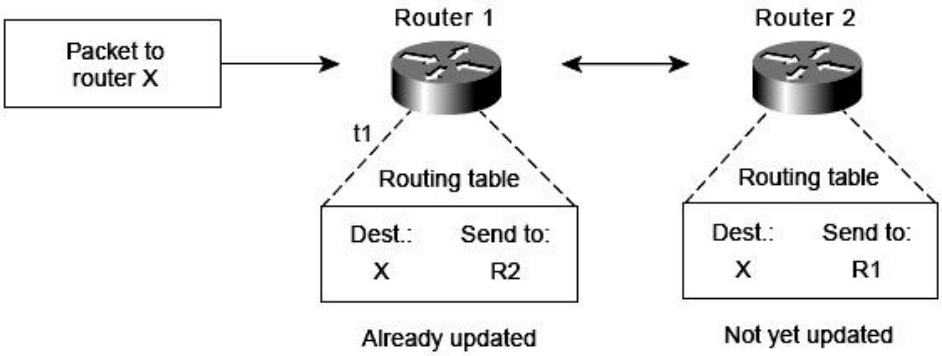


Fig. Destination/Next Hop Associations Determine the Data's Optimal Path

Routing tables also can contain other information, such as data about the desirability of a path. Routers compare metrics to determine optimal routes, and these metrics differ depending on the design of the routing algorithm used.

Routers communicate with one another and maintain their routing tables through the transmission of a variety of messages. The routing update message is one such message that generally consists of all or a portion of a routing table. By analyzing routing updates from all other routers, a router can build a detailed picture of network topology. A link-state advertisement, another example of a message sent between routers, informs other routers of the state of the sender's links. Link information also can be used to build a complete picture of network topology to enable routers to determine optimal routes to network destinations.

12.2 SWITCHING

Switching algorithms is relatively simple; it is the same for most routing protocols. In most cases, a host determines that it must send a packet to another host. Having acquired a router's address by some means, the source host sends a packet addressed specifically to a router's physical (Media Access Control [MAC]-layer) address, this time with the protocol (network layer) address of the destination host.

As it examines the packet's destination protocol address, the router determines that it either knows or does not know how to forward the packet to the next hop. If the router does not know how to forward the packet, it typically drops the packet. If the router knows how to forward the packet, however, it changes the destination physical address to that of the next hop and transmits the packet. The next hop may be the ultimate destination host. If not, the next hop is usually another router, which executes the same switching decision process. As the packet moves through the

internetwork, its physical address changes, but its protocol address remains constant.

The preceding discussion describes switching between a source and a destination end system. The International Organization for Standardization (ISO) has developed a hierarchical terminology that is useful in describing this process. Using this terminology, network devices without the capability to forward packets between subnetworks are called *end systems (ESs)*, whereas network devices with these capabilities are called *intermediate systems (ISs)*. ISs are further divided into those that can communicate within routing domains (*intradomain ISs*) and those that communicate both within and between routing domains (*interdomain ISs*). A routing domain generally is considered a portion of an internetwork under common administrative authority that is regulated by a particular set of administrative guidelines. Routing domains are also called autonomous systems.With certain protocols, routing domains can be divided into routing areas, but intradomain routing protocols are still used for switching both within and between areas.

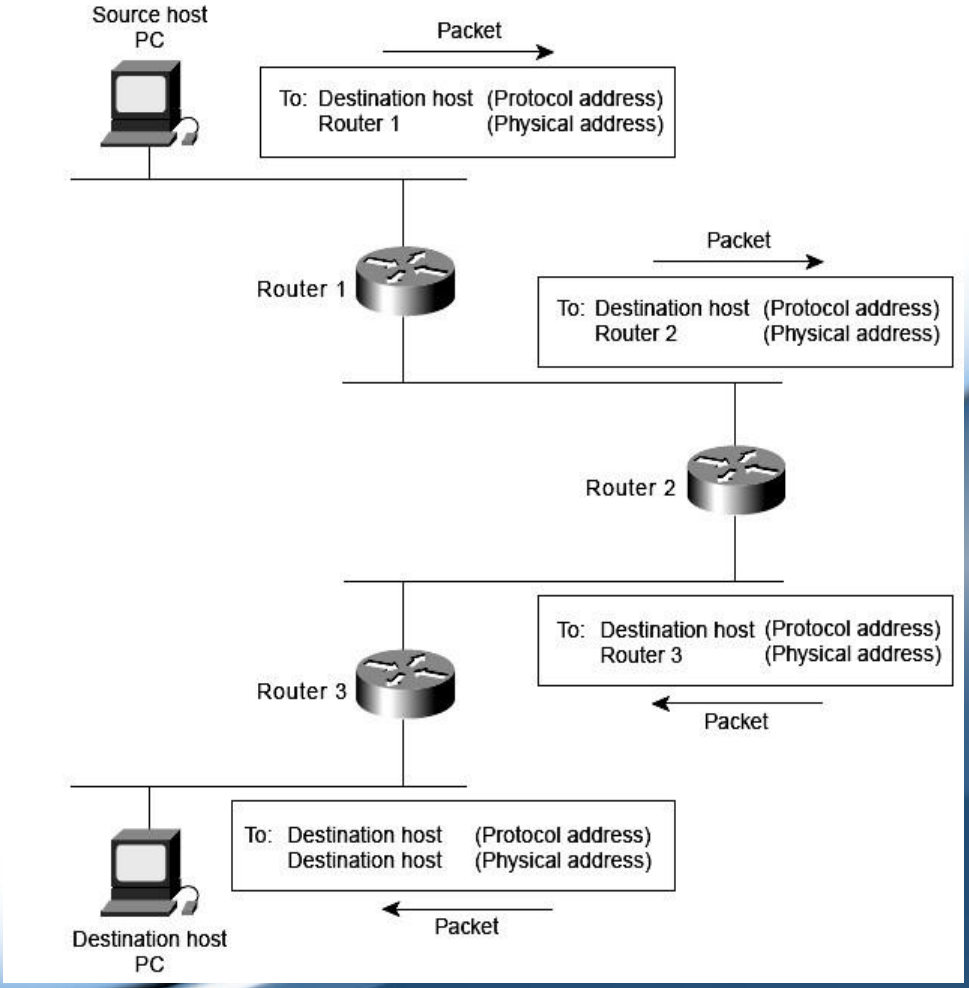


Fig.of switching

12.3 INTRODUCTION TO ALGORITHM

Routing Algorithms- Introduction

Routing algorithms can be differentiated based on several key characteristics. First, the particular goals of the algorithm designer affect the operation of the resulting routing protocol. Second, various types of routing algorithms exist, and each algorithm has a different impact on network and router resources.

Finally, routing algorithms use a variety of metrics that affect calculation of optimal routes. The following sections analyze these routing algorithm attributes.

*12.3.1*Design Goals

Routing algorithms often have one or more of the following design goals:

• Optimality

• Simplicity and low overhead

• Robustness and stability

• Rapid convergence

• Flexibility

- *Optimality* refers to the capability of the routing algorithm to select the best route, which depends on the metrics and metric weightings used to make the calculation.

For example, one routing algorithm may use a number of hops and delays, but it may weigh delay more heavily in the calculation. Naturally, routing protocols must define their metric calculation algorithms strictly.

- Routing algorithms also are designed to be as simple as possible. In other words, the routing algorithm must offer its functionality efficiently, with a minimum of software and utilization overhead. Efficiency is particularly important when the software implementing the routing algorithm must run on a computer with limited physical resources.

- Routing algorithms must be *robust*, which means that they should perform correctly in the face of unusual or unforeseen circumstances, such as hardware failures, high load conditions, and incorrect implementations. Because routers are located at network junction points, they can cause considerable problems when they fail. The best routing

algorithms are often those that have withstood the test of time and that have proven stable under a variety of network conditions.

- In addition, routing algorithms must converge rapidly. *Convergence* is the process of agreement, by all routers, on optimal routes. When a network event causes routes to either go down or become available, routers distribute routing update messages that permeate networks, stimulating recalculation of optimal routes and eventually causing all routers to agree on these routes. Routing algorithms that converge slowly can cause routing loops or network outages.

- Routing algorithms should also be flexible, which means that they should quickly and accurately adapt to a variety of network circumstances. Assume, for example, that a network segment has gone down. As many routing algorithms become aware of the problem, they will quickly select the next-best path for all routes normally using that segment. Routing algorithms can be programmed to adapt to changes in network bandwidth, router queue size, and network delay, among other variables.

- **12.3.2 Routing Algorithm Types**

Routing algorithms can be classified by type. Key differentiators include these:

1. Static versus dynamic
2. Single-path versus multipath
3. Flat versus hierarchical
4. Host-intelligent versus router-intelligent
5. Intradomain versus interdomain
6. Link-state versus distance vector

1. Static Versus Dynamic

Static routing algorithms are hardly algorithms at all, but are table mappings established by the network administrator before the beginning of routing. These mappings do not change unless the network administrator alters them. Algorithms that use static routes are simple to design and work well in environments where network traffic is relatively predictable and where network design is relatively simple.

Because static routing systems cannot react to network changes, they generally are considered unsuitable for today‘s large, constantly changing networks. Most of the dominant routing algorithms today are

Dynamic routing algorithms, which adjust to changing network circumstances by analyzing incoming routing update messages. If the message indicates that a network change has occurred, the routing software recalculates routes and sends out new routing update messages. These messages permeate the network, stimulating routers to rerun their algorithms and change their routing tables accordingly.

Dynamic routing algorithms can be supplemented with static routes where appropriate. A router of last resort (a router to which all unroutable packets are sent), for example, can be designated to act as a repository for all unroutable packets, ensuring that all messages are at least handled in some way.

2. Single-Path Versus Multipath

Some sophisticated routing protocols support multiple paths to the same destination. Unlike single-path algorithms, these multipath algorithms permit traffic multiplexing over multiple lines. The advantages of multipath algorithms are obvious: They can provide substantially better throughput and reliability. This is generally called load sharing.

3. Flat Versus Hierarchical

Some routing algorithms operate in a flat space, while others use routing hierarchies.

In a *flat routing system*, the routers are peers of all others. In a hierarchical routing system, some routers form whatamounts to a routing backbone. Packets from nonbackbone routers travel to the backbone routers, wherethey are sent through the backbone until they reach the general area of the destination. At this point, theytravel from the last backbone router through one or more nonbackbone routers to the final destination.Routing systems often designate logical groups of nodes, called domains, autonomous systems, or areas.

In *hierarchical systems*, some routers in a domain can communicate with routers in other domains, while others can communicate only with routers within their domain. In very large networks, additional hierarchical levels may exist, with routers at the highest hierarchical level forming the routing backbone.

The primary advantage of hierarchical routing is that it mimics the organization of most companies and therefore supports their traffic patterns well. Most network communication occurs within small company groups (domains). Because intradomain routers need to know only about other routers within their domain, their routing algorithms can be simplified, and, depending on the routing algorithm being used, routing update traffic can be reduced accordingly.

4. Host-Intelligent Versus Router-Intelligent

Some routing algorithms assume that the source end node will determine the entire route. This is usually referred to as *source routing*. In source-routing systems, routers merely act as store-and-forward devices, mindlessly sending the packet to the next stop.

Other algorithms assume that hosts know nothing about routes. In these algorithms, routers determine the path through the internetwork based on their own calculations. In the first system, the hosts have the routing intelligence. In the latter system, routers have the routing intelligence.

5. Intradomain Versus Interdomain

Some routing algorithms work only within domains; others work within and between domains. The nature of these two algorithm types is different. It stands to reason, therefore, that an optimal intradomain-routing algorithm would not necessarily be an optimal interdomain-routing algorithm.

6. Link-State Versus Distance Vector

Link-state algorithms (also known as shortest path first algorithms) flood routing information to all nodes in the internetwork. Each router, however, sends only the portion of the routing table that describes the state of its own links. In link-state algorithms, each router builds a picture of the entire network in its routing tables.

Distance vector algorithms (also known as Bellman-Ford algorithms) call for each outer to send all or some portion of its routing table, but only to its neighbors. In essence, link-state algorithms send small updates everywhere, while distance vector algorithms send larger updates only to neighboring routers. *Distance vector* algorithms know only about their neighbors. Because they converge more quickly, link-state algorithms are somewhat less prone to routing loops than distance vector algorithms. On the other hand, link-state algorithms require more CPU power and memory than distance vector algorithms. Link-state algorithms, therefore, can be more expensive to implement and support. Link-state protocols are generally more scalable than distance vector protocols.

12.4 ROUTING METRICS

Routing tables contain information used by switching software to select the best route. Routing algorithms have used many different metrics to determine the best route. Sophisticated routing algorithms can base route selection on multiple metrics, combining them in a single (hybrid) metric. All the following metrics have been used:

- Path length
- Reliability
- Delay
- Bandwidth Load
- Communication cost

- *Path length* is the most common routing metric. Some routing protocols allow network administrators to assign arbitrary costs to each network link. In this case, path length is the sum of the costs associated with each link traversed. Other routing protocols define hop count, a metric that specifies the number of passes through internetworking products, such as routers, that a packet must take en route from a source to a destination.

- *Reliability*, in the context of routing algorithms, refers to the dependability (usually described in terms of the bit-error rate) of each network link. Some network links might go down more often than others. After a network fails, certain network links might be repaired more easily or more quickly than other links. Any reliability factors can be taken into account in the assignment of the reliability ratings, which are arbitrary numeric values usually assigned to network links by network administrators.

- *Routing delay* refers to the length of time required to move a packet from source to destination through the internetwork. Delay depends on many factors, including the bandwidth of intermediate network links, the port queues at each router along the way, network congestion on all intermediate network links, and the physical distance to be travelled. Because delay is a conglomeration of several important variables, it is a common and useful metric.

- *Bandwidth* refers to the available traffic capacity of a link. All other things being equal, a 10-Mbps Ethernet link would be preferable to a 64-kbps leased line. Although bandwidth is a rating of the maximum attainable throughput on a link, routes through links with greater bandwidth do not necessarily provide better routes than routes through slower links. For example, if a faster link is busier, the actual time required to send a packet to the destination could be greater.

- *Load* refers to the degree to which a network resource, such as a router, is busy. Load can be calculated in a variety of ways, including CPU utilization and packets processed per second. Monitoring these parameters on a continual basis can be resource-intensive itself.

- *Communication cost* is another important metric, especially because some companies may not care about performance as much as they care about operating expenditures. Although line delay may be longer, they will send packets over their own lines rather than through the public lines that cost money for usage time.

12.5 SUMMARY

- *Routing* is the act of moving information across an internetwork from a source to a destination.
- Routing involves two basic activities: determining optimal routing paths and transporting information groups (typically called packets) through an internetwork.
- Routing protocols use metrics to evaluate what path will be the best for a packet to travel.
- Routing protocols use metrics to evaluate what path will be the best for a packet to travel.
- Switching algorithms is relatively simple; it is the same for most routing protocols.
- Routing algorithms often have one or more of the following design goals:
  - Optimality
  - Simplicity and low overhead
  - Robustness and stability
  - Rapid convergence
  - Flexibility

- Routing tables contain information used by switching software to select the best route.

6. REVIEW QUESTION

1. Explain routing concept?
2. Explain switching concept?
3. Discuss design goal?
4. Explain routing algorithms?
5. Explain Routing metrics?

12.6 LIST OF REFERENCES

- Stamper, D. (1993) *Local Area Networks*, Addison-Wesley, Reading, MA.
- Stamper, D. (1991) *Business Data Communications*, Third Edition, Addison-Wesley, Reading, MA.
- Stone, H. (1982), *Microcomputer Interfacing*, Addison-Wesley, Reading, MA.
- Tanenbaum, A. (1989), *Computer Networks*, Second Edition, Prentice Hall, Englewood Cliffs, NJ.
- Van Duuren, J., Schoute, F., and Kastelein, P. (1992) *Telecommunications*
- *Networks and Services*, Addison-Wesley, Reading, MA.
- Viniotis Y. and Onvural R. (editors) (1993) *Asynchronous Transfer Mode, Networks*, Plenum, New York, NY.
- White, G. (1992) *Internetworking and Addressing*, McGraw-Hill, NY.
- Zitsen, W. (1990) ‗Metropolitan Area Networks: Taking LANs into the Public, Network,' *Telecommunications*, pp. 53-60.

13

SWITCHING CONCEPTS

Unit Structure

13.0 OBJECTIVE

- ✓ Introduce switching concept
- ✓ Define switching node
- ✓ Define packet switching
- ✓ Switching mode

13.1 INTRODUCTION

Switching is the generic method for establishing a path for point-to-point communication in a network. It involves the nodes in

the network utilizing their direct communication lines to other nodes so that a path is established in a piecewise fashion. Each node has the capability to „switch‘ to a neighbouring node (i.e., a node to which it is directly connected) to further stretch the path until it is completed.

One of the most important functions of the network layer is to employ theswitching capability of the nodes in order to route messages across the network.There are two basic methods of switching circuit switching and packet switching.

13.2.1. Circuit Switching

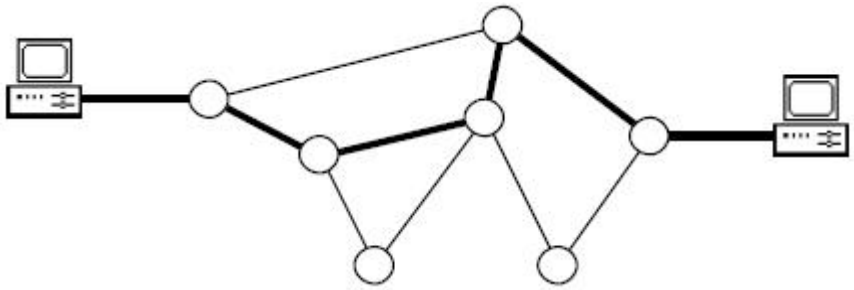


Figure 13.2.1 A „switched" path.

In circuit switching, two communicating stations are connected by a *dedicated* communication path which consists of intermediate nodes in the network and thelinks that connect these nodes.

Figure **13.2.1** shows a simple circuit switch which consists of a 3×3 matrix, capable of connecting any of its inlets (*a*, *b*, and *c*) to any of its outlets (*d*, *e*, and *f*). Each crosspoint appears as a circle. A hollow circle means that the crosspoint is *off* (i.e., the two crossing wires are not connected). A solid circles means that the crosspoint is *on* (i.e., the crossing wires are connected).

Switches may also have more inlets than outlets, or more outlets than inlets.)

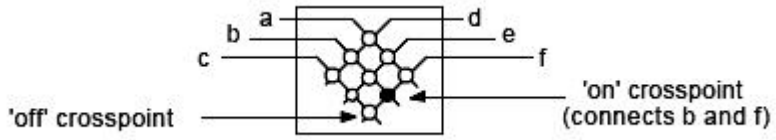


Figure 13.2.2 A simple circuit switch.

When the two hosts shown in the figure initiate a connection, the network determines a path through the intermediate switches and establishes a circuit which is maintained for the duration of the connection. When the hosts disconnect, the network releases the circuit.

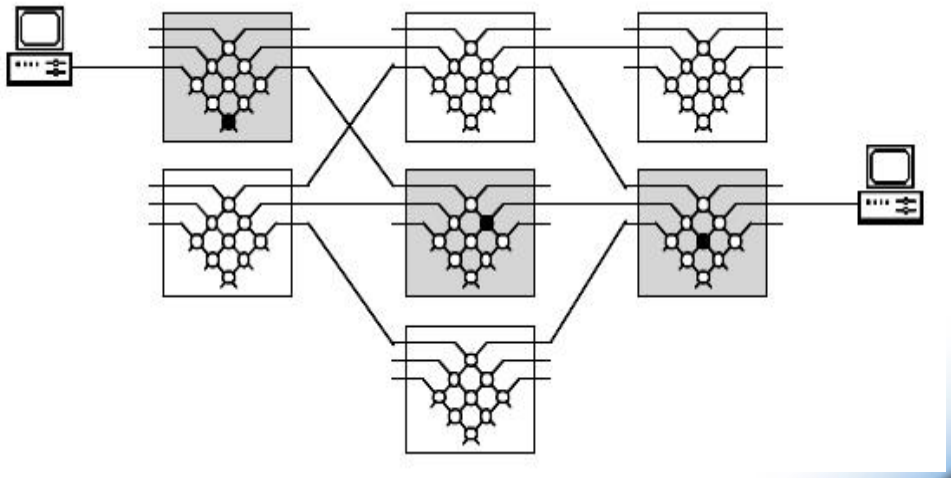


Fig 13.2.3 Circuit switching.

Communication via circuit switching implies that there is a dedicated communication path between the two stations. The path is a connected through a sequence of links between network nodes. On each physical link, a logical channel is dedicated to the connection. Circuit switching is commonly used technique in telephony, where the caller sends a special message with the address of the callee (i.e. by dialling a number) to state its destination. It involved the following three distinct steps, as shown in Fig. **13.2.3**

Circuit Establishment: To establish an end-to-end connection before any transfer of data.

Some segments of the circuit may be a dedicated link, while some other segments may be shared.

Data transfer:

Transfer data is from the source to the destination.
The data may be analog or digital, depending on the nature of the network.
The connection is generally full-duplex.

Circuit disconnect:

Terminate connection at the end of data transfer.

• Signals must be propagated to deallocate the dedicated resources.

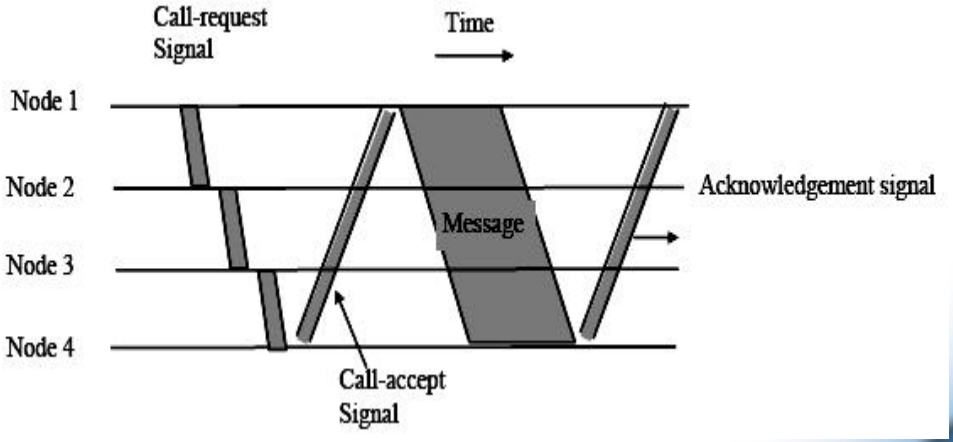


Fig: 13.2.4 Circuit Switching technique

13.2.2 Switching Node

Let us consider the operation of a single circuit switched node comprising a collection of stations attached to a central switching unit, which establishes a dedicated path between any two devices that wish to communicate.

Major elements of a single-node network are summarized below:

***Digital switch*:** That provides a transparent (full-duplex) signal path between any pair of attached devices.

Network interface:That represents the functions and hardware needed to connect digital devices to the network (like telephones).

Control unit:That establishes, maintains, and tears down a connection.

An important characteristic of a circuit-switch node is whether it is *blocking* or *non-blocking*.

A blocking network is one, which may be unable to connect two stations because all possible paths between them are already in use. A non-blocking network permits all stations to be connected (in pairs) at once and grants all possible connection requests as long as the called party is free. For a network that supports only voice traffic, a blocking configuration may be acceptable, since most phone calls are of short duration. For data applications, where a connection may remain active for hours, non-blocking configuration is desirable.

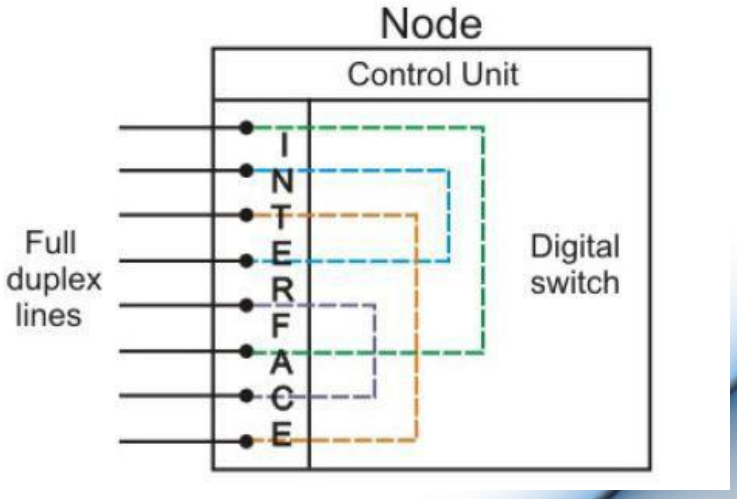


Fig 13.2.5 Schematic Diagram of a Switching node

Circuit switching uses any of the three technologies: **Space-division** switches, **Time-division** switches or a **combination of both**. In Space-division switching, the paths in the circuit are separated with each other spatially, i.e. different ongoing connections, at a same instant of time, uses different switching paths, which are separated spatially. This was originally developed

Thank You