UNIT 3 INTRODUCTION TO NETWORKING CONCEPT

Structure **Page Nos.**

3.0 INTRODUCTION

A network can consist of two computers connected together on a desk or it can consist of many Local Area Networks (LANs) connected together to form a Wide Area Network (WAN) across a continent. In simple terms it is an interconnected set of some objects. For decades, we have been familiar with the Radio, Television, Railways, Banks and various other types of networks. In recent years, the computer network, a new form of network is becoming more and more visible in our day-to-day life. A computer network is an interconnected set of autonomous computers.

Autonomous means each of them can function independent of others, i.e., each computer has individual processors. Simply we can say each computer (terminal, node) should not be a dump terminal. The key is that two or more computers are connected together by a medium and are sharing resources. These resources can be files, printers, hard drives, CPU or data. By using a computer network, people can send and receive back information more quickly.

3.1 OBJECTIVES

After going through this unit, you should be able to:

- define what a network is?
- understand what is the need of a computer network and the applications of networks;
- list types of networks, topologies and mediums finally, and
- how devices are connected though repeater, bridges, router, Gateway.

3.2 WHY COMPUTER NETWORKS?

Computer Networks offer a number of advantages to individuals and organization. Some of these are:

a) **Communication medium**: It offers a powerful communication medium among a group of people widely separated on the earth.

b) **Resource Sharing**: Resources like files, printers, hard drives, or CPU can be shared through a computer network.

c) **Higher Reliability:** If one computer **is** down; its workload can be taken over by the other computer. So it offers higher reliability than a centralized computing environment.

d) **Higher flexibility**: A heterogeneous system can be connected in a computer network, by which users get better flexibility.

e) **Scalable:** Computers and other equipments can be gradually added to satisfy the need of an organisation at different points of time, without changing the original network.

Applications of computer network

a) **Electronic Mail** (e-mail or Email). The most widely used network application is E-mail, which is forwarding of electronic files to an electronic post office for the recipient to pick up.

b) Scheduling programs allow people across the network to schedule appointments directly by calling up their fellow worker's schedule and selecting a time!

c) Videotext is the capability of having a two-way transmission of picture and sound. Games like distance education lectures, etc. use videotext.

d) Groupware is the latest network application. It allows user groups to share documents, schedules databases

e) Teleconferencing allows people in different regions to "attend" meetings using telephone lines.

f) Automated Banking Machines allow banking transactions to be performed everywhere: at grocery stores, drive-in machines etc.

g) Information Service Providers provide connections to the Internet and other information services.

h) Telecommuting allows employees to perform office work at home by "Remote Access" to the network.

i) Value Added Networks are common carriers such as ERNET, Satyam ,VSNL etc. (they can be private or public companies) who provide additional leased line

connections to their customers. These can be Frame Relay, ATM (Asynchronous Transfer Mode), X.25, etc.

(j) Marketing and sales Marketing professionals use computer network to collect, exchange and analyse data relating to customer needs.

3.3 THE TOPOLOGIES

The topology is the geometric arrangement (either physically or logically) of the linking devices (usually called nodes) and the links, connecting the individual computers or nodes together. Five basic topologies:

1) Bus topology

2) Ring topology

3) Star topology

4) Mesh topology

5) Combined topologies.

1) **The Bus Topology**

In the bus topology there is a single bus that carries all the data to the entire network. A bus is a single continuous communication cable to which all the computers are connected. A cable or bus runs throughout the office to which all the workstations are connected. The bus topology is also known as *linear bus.*

When one workstation wants to talk to another the message or signal travels down the bus in both directions. Each one reads the message to see if it matches its address. The bus topology is a passive topology. It means that the computers connected to the bus amplify the signal on the bus.

The main advantage of bus topology is that it is quite easy to set up. Any workstation can be easily moved to another location as bus runs throughout the office. Another benefit of this layout is that if one computer on the bus fails, it does not affect the rest of the traffic on the bus.

A network with bus topology cannot become too big as all the traffic is on a single bus. The entire network can be down only if the bus has a break. The open ends of bus must be terminated to prevent signal bounce. If one or both ends of the bus are not terminated, the whole network can be down.

Disadvantages include difficult reconfiguration and fault isolation

2) **The Ring Topology**

In the ring topology all the workstations are connected in the shape of a ring. The ring does not have an end. It is made up of short segments that connect one PC to the next and so on, until all the computers are joined in a circle. The signals travel only in one direction and from one PC to the next until it reaches the appropriate node. It is also difficult to move a workstation or to add more computers to an existing ring.

In ring topology the wiring for a ring could be arranged in a circle throughout a building or a group of buildings. The signal travels in one direction only from one computer to the next. The ring topology is an active topology. Each computer boosts the signal (like a repeater) and passes to the next computer till it reaches the destination computer. A drawback of this topology is that if one computer fails, the entire network is down. However, now some ring networks are so designed that a faulty workstation is automatically bypassed. Another drawback is that the traffic is in only one direction. This topology is not used for a large number of nodes.

3) The Star Topology

In the star topology all the stations are connected to a central computer or hub creating a star configuration. The devices are not directly linked to each other Messages pass from the nodes to the hub, where they are processed or passed along to another node. The hub controls the traffic on the network. If the hub fails, the entire network becomes inoperative, but if a node fails it does not affect the rest of the traffic on the network.

All client/server networks use this topology. But since cable from each node must be connected to a central hub, the length of total wiring required increases very much. A hub can be an active hub or a passive hub. A passive hub simply organizes the wiring and works just like a wiring panel for various connections. It does not need any power connection. An active hub does what a passive hub does, but besides this it regenerate and retransmits the signals the way a repeater does. An active hub needs a power connection.

4) Mesh Topology

In a mesh topology, every node has a dedicated point-to point link to every other node. Simply dedicated means that the links carry traffic only between the two nodes. So mesh topology does not have traffic congestion problems every node has n-1 link,for a fully connected mesh topology having n nodes. So the total number of links will be n (n-1).This also means that every node has (n-1) I/O ports.

Advantages of Mesh topology

1) Use of dedicated links guarantees that each connection can carry its own data load. Thus eliminates the traffic problem.

2) If one link fails, it does not affect the rest of network. This means it is robust.

3) Point to point links make fault identification and fault isolation easy.

4) Privacy or security is high, since the other link cannot gain access to the dedicated link where the message is travelling.

Disadvantages of mesh topology

1) More cabling and I/O ports are required, because every node must be connected to every other node.

2) Cost is very high, because more number of node and cabling required.

3) Installation and reconfiguration is difficult.

5) Combined Topologies

A network does not have to stick with one topology. Any two topologies or all the topologies can be used in a network. For example, a hub may be connected to other hubs using a bus and the workstations may be connected by a star.

Two main hybrid topologies are:

1) The Star Bus Topology

The star bus topology is a combination of bus and star topologies. In this topology the hubs of many star topology networks are linked together with a linear bus or trunk. For example, we want to link three star topology networks together. In each network, the nodes are connected to its own hub. Thus we have three hubs. These three hubs are connected by a bus topology.

2) The Star Ring Topology

In this topology the hubs of many star topology networks are connected to another main hub in a star pattern. Thus if we have three star topology networks, then the three hubs of the networks are connected to a fourth hub (main hub) in star pattern.

3.4 CHARACTERISTICS OF THE OSI LAYERS

There are primarily two architectural models for designing computer networks. OSI model & TCP/IP model. In this section we shall discuss one such model.

The seven layers of the OSI reference model can be divided into two categories: upper layers and lower layers.

The *upper layers* of the OSI model deal with application issues and generally are implemented only in software. The highest layer, the application layer, is closest to the end user. Both users and application layer processes interact with software applications that contain a communications component. The term upper layer is sometimes used to refer to any layer above another layer in the OSI model.

The *lower layers* of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical layer, is closest to the physical network medium (the network cabling, for example) and is responsible for actually placing information on the medium.

Figure 1 illustrates the division between the upper and lower OSI layers.

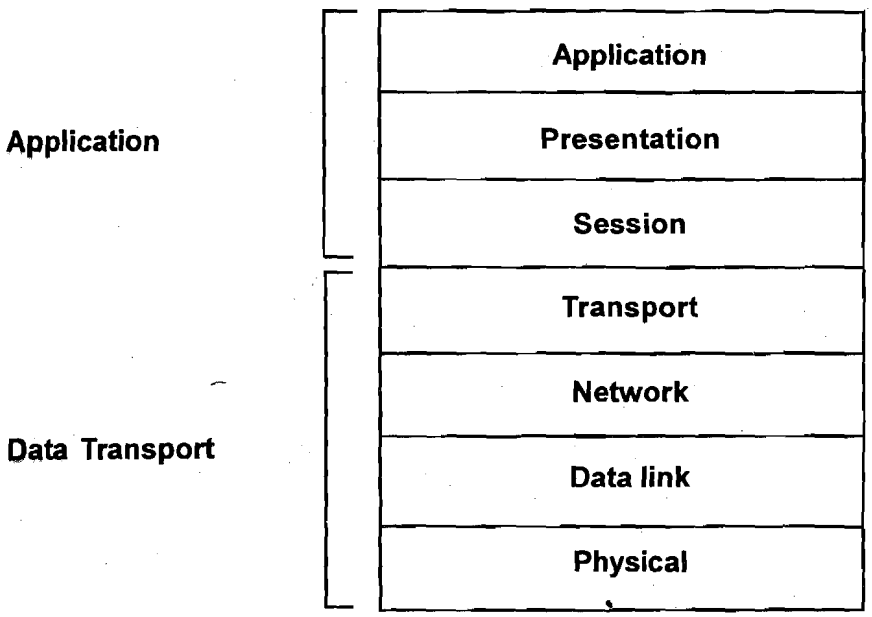

Figure 1: Two Sets of Layers Make Up the OSI Layers

Each layer has well defined functionalities and standard protocols for implementing thes functionalities.

3.5 OSI MODEL AND COMMUNICATION BETWEEN SYSTEMS

Information being transferred from a software application in one computer system to a software application in another must pass through the OSI layers. For example, if a software application in System A has information to transmit to a software application

in System B, the application program in System A will pass its information to the application layer (Layer 7) of System A. The application layer then passes the information to the presentation layer (Layer 6), which relays the data to the session layer (Layer 5), and so on down to the physical layer (Layer 1). At the physical layer, the information is placed on the physical network medium and is sent across the medium to System B. The physical layer of System B removes the information from the physical medium, and then its physical layer passes the information up to the data link layer (Layer 2), which passes it to the network layer (Layer 3), and so on, until it reaches the application layer (Layer 7) of System B. Finally, the application layer of System B passes the information to the recipient application program to complete the communication process.

3.6 INTERACTION BETWEEN OSI MODEL LAYERS

A given layer in the OSI model generally communicates with three other OSI layers: the layer directly above it, the layer directly below it, and its peer layer in other networked computer systems. The data link layer in System A, for example, communicates with the network layer of System A, the physical layer of System A, and the data link layer in System B. *Figure 2* illustrates this example.

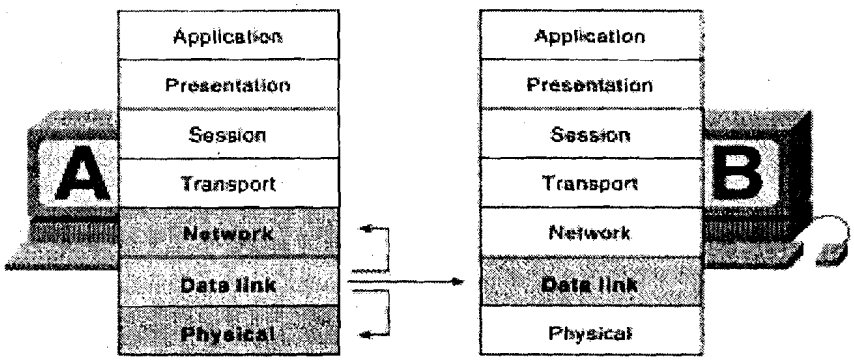

Figure 2: OSI Model Layers Communicate with Other Layers

3.7 PROTOCOLS

Just like human beings need to have a common languages to speak to one another, digital devices and computers also need to have common 'languages' to be able to communicate with one another. The binding function of 'common language' in digital communication is performed by communication protocols.

A communication protocol is a set of conventions or rules that must be adhered to by both communicating parties to ensure that information being exchanged between two parties is received and interpreted correctly. Without a protocol, two devices may be connected but not communicating, just as a person speaking Hindi cannot be understood by a person who speaks only Tamil.

A protocol defines the following three aspects of communication.

1) **Syntax:** The format of data being exchanged, character set used, type of error correction used, type of encoding scheme (e.g., signal level) being used. For example, a simple protocol may use first eight bit for address of sender, the second eight bit for address of receiver and the rest of bit for message itself.

2) **Semantics:** Type and order of messages used to ensure reliable and error free information transfer.

3) **Timing:** Define data rate selection and correct timing for various events during data transfer. Simply when data should be sent and how fast they can be sent.

It has been accepted that the complexity of writing communication software can be reduced by adapting the principle of protocol layering. The idea here is to partition communication functions into a vertical set of layers. Each layer performs a related set of functions. Division of work between layers is done in such a way that they are manageable and provide a logical interface and break point. Each communication layer provides certain services to layers above it and relies on the next lower layer to perform more primitive functions. Each layer hides internal details from other layers. Thus dividing the communication problem into several layers reduces its complexity and makes the work of developing communication software a lot easier and error free.

3.8 TYPES OF NETWORKS

The differences among different types of computer networks are usually based on perspective. For example, computer networks are frequently classified by the geographical area (LAN, MAN, WAN), their topologies (e.g., point to point or broadcast),or the type of communication path they use and the manner in which data are transmitted across this path (e.g., circuit-switched and packet-switched).

Computer networks are classified by the geographical area are:

1) Local Area Networks (LANs)

2) Metropolitan Network (MANs)

3) Wide Area Networks (WANs)

3.8.1 Local Area Networks (LANs)

LANs (local area networks), as shown in *Figure 3* are privately-owned networks that connect computers and resources together in a building or buildings that are close together. LAN plays an important part in everyday functioning of schools, businesses, and government.

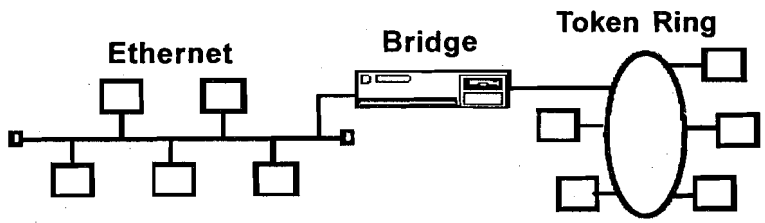

Figure3: Local Area Network in a building

A *LAN* is a high-speed data network that covers a relatively small geographic area. It typically connects workstations, personal computers, printers, servers, and other devices, so that devices can communicate with each other to share resources. LANs offer computer users many advantages, including shared access to devices and applications, file exchange between connected users, and communication between users via electronic mail and other applications.

A Local Area Network is a system of computers that share resources such as disk drives, printers, data, CPU power, fax/modem, applications, etc. They usually have distributed processing, which means that there are many desktop computers distributed around the network and that there is no central processor machine (mainframe).

Location: In a building or individual rooms or floors of buildings or nearby buildings. Can be campus wide like a college or university.

LAN Characterisation

There are four key areas that characterise a local area network.

These are:

1) Transmission Medium
2) Access Method
3) Topology
4) Signaling Techniques

LAN Media-Access Methods

Media contention occurs when two or more network devices have data to send at the same time. Because multiple devices cannot talk on the network simultaneously, some type of method must be used to allow one device access to the network media at a time. This is done in two main ways: carrier senses multiple accesses collision detect (CSMA/CD) and token passing.

In networks using CSMA/CD technology such as Ethernet, network devices contend for the network media. When a device has data to send, it first listens to see if any other device is currently using the network. If not, it starts sending its data. After finishing its transmission, it listens again to see if a collision occurred. A collision occurs when two devices send data simultaneously. When a collision happens, each device waits a random length of time before resending its data. In most cases, a collision will not occur again between the two devices. Because of this type of network contention, the busier a network becomes, the more collisions occur. This is why performance of Ethernet degrades rapidly as the number of devices on a single network increases.

In token-passing networks such as Token Ring and FDDI, a special network packet called a token is passed around the network from device to device. When a device has data to send, it must wait until it has the token and then send its data. When the data transmission is complete, the token is released so that other devices may use the network media. The main advantage of token-passing networks is that they are deterministic. In other words, it is easy to calculate the maximum time that will pass before a device has the opportunity to send data. This explains the popularity of token-passing networks in some real-time environments such as factories, where machinery must be capable of communicating at determinable intervals.

For CSMA/CD networks, switches segment the network into multiple collision domains. This reduces the number of devices per network segment that must contend for the media. By creating smaller collision domains, the performance of a network can be increased significantly without requiring addressing changes.

Normally CSMA/CD networks are half-duplex, meaning that while a device sends information, it cannot receive at the same time. While that device is talking, it is incapable of also listening for other traffic. This is much like a walkie-talkie. When one person wants to talk, he presses the transmit button and begins speaking. While he is talking, no one else on the same frequency can talk. When the sending person is finished, he releases the transmit button and the frequency is available to others.

When switches are introduced, full-duplex operation is possible. Full-duplex works much like a telephone—you can listen as well as talk at the same time. When a network device is attached directly to the port of a network switch, the two devices may be capable of operating in full-duplex mode. In full-duplex mode, performance can be increased, but not quite as much as some like to claim.. However, full-duplex operation does increase the throughput of most applications because the network

media is no longer shared. Two devices on a full-duplex connection can send data as soon as it is ready.

Token-passing networks such as Token Ring can also benefit from network switches. In large networks, the delay between turns to transmit may be significant because the token is passed around the network.

LAN Transmission Methods

For Transmission, LAN usually broadcast their message to all hosts on the LAN The address in the packet or frame enables the destination to receive the packet, while the rest of the hosts ignore the broadcast message.

LAN data transmissions fall into three classifications: unicast, multicast, and broadcast. In each type of transmission, a single packet is sent to one or more nodes.

In a unicast transmission, a single packet is sent from the source to a destination on a network. First, the source node addresses the packet by using the address of the destination node. The package is then sent onto the network, and finally, the network passes the packet to its destination.

A multicast transmission consists of a single data packet that is copied and sent to a specific subset of nodes on the network. First, the source node addresses the packet by using a multicast address. The packet is then sent into the network, which makes copies of the packet and sends a copy to each node that is part of the multicast address.

A broadcast transmission consists of a single data packet that is copied and sent to all nodes on the network. In these types of transmissions, the source node addresses the packet by using the broadcast address. The packet is then sent on to the network, which makes copies of the packet and sends a copy to every node on the network

Topology: The most common LAN topologies are bus, ring, and star.

3.8.2 Metropolitan Networks (MANs)

Metropolitan Area Networks (MANs), as shown in *Figure 4*, are networks that connect LANs together within a city.

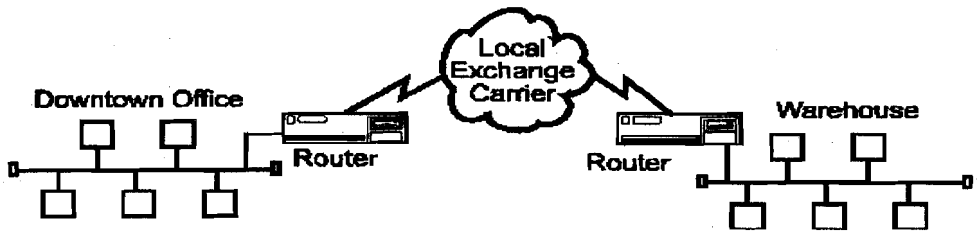

Figure 4: MANs use Local Exchange Carriers

The main criterion for a MAN is that the connection between LANs is through a local exchange carrier (the local phone company) . The protocols that are used for MANs are quite different from those used for LANs (except for ATM, which can be used for both under certain conditions). It has been distinguished as a separate type of network; because of the specific standard known as Distributed Queue Double Bus (DQDB) that has been adopted for MAN. The DQDB comprises two unidirectional buses for connecting computers.

A Metropolitan Area Network is a system of LANs connected throughout a city (*Figure 5*) or metropolitan area. MAN can be considered as a bigger version of a

LAN, typically covering a city. It can be either public or privately owned. MANs have the requirement of using telecommunication media such as voice channels or data channels. Branch offices are connected to head offices through MANs. Examples of organizations that use MANs are universities and colleges, hotels, and banks.

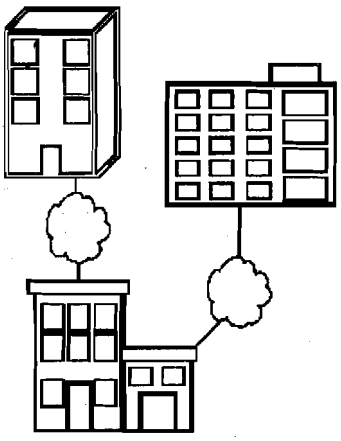

Figure 5: Location: Separate buildings distributed throughout a city

3.8.3 Wide Area Networks (WANs)

Wide Area Networks (WANs) connect LANs together between cities (*Figure 6*).

Communication is usually done through public communication systems such as telephone line, fiber optic cable or wireless technology.

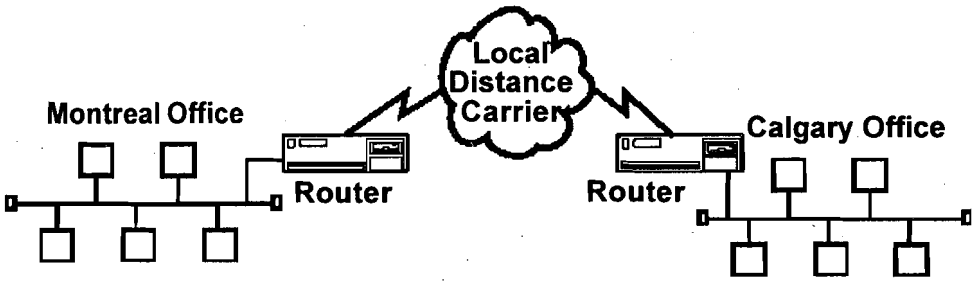

Figure 6: WANs use Long Distance Carriers

A Wide Area Network is a network system connecting cities, countries, or continents together *Figure 7*. WANs are connected together using one of the telecommunications media.

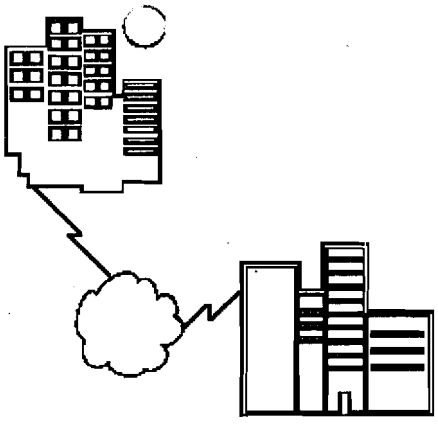

Figure 7: City to city, across a country or across a continent.

The main difference between a MAN and a WAN is that the WAN uses Long Distance Carriers. Otherwise the same protocols and equipment are used as in MAN.

Main differences between a LAN and a WAN are given in the following Table1.

Table1: Difference between LAN and MAN

Wide area Network	Local Area Network
Distance up to thousands of Kilometer	Within a local site
Typical data rates between 9.6k to 1Mbps	High band width between 1-16 Mbps
Higher error rates (1 in 10^5)	Lower error rate (1 in 10^9)
Often use analog circuits from the telephone systems	Use digital signaling over private cables
	Generally use bus or ring topology
Generally has point–to-point link with common topologies mesh and star	Managed by the same company which owns the computers connected to LAN
May be managed by organizations independent of users	LAN uses simple protocols and does not employ any retransmission strategy for lost frames
WAN uses complex protocols and extensive error recovery mechanisms	Number of host on a LAN is limited (usually up to 1024)
Number of node computers has no theoretical limit and could be very large. The practical limit comes from addressing schemes used to identify individual system on the network and other resource constrains.	

3.9 MEDIUM

Data communication system is made up of following components (*Figure 8*).

Figure 8: Data Communication-I

Source Sender: Sender can be Terminals, Computers, Mainframes, workstation, telephone hand set, video camera. Main function of sender is to send data (message) to receiver.

The communications stream through which the data is being transmitted. Examples are:

- Cables
- Microwave Link
- Fiber optic Link
- Radio Frequencies (RF)
- Infrared Wireless

Receiver: The receiver receives the message (data) from sender. Receiver can be Terminals, Computers, Mainframes, workstation, telephone hand set, printer, television and so on.

Protocol: A communication protocol is a set of conventions or rules that must be adhered to by both communicating parties to ensure that information being exchanged between two parties is received and interpreted correctly.

Message: Message consists of text, numbers, pictures, sound, or video – or any combination of these to be transmitted from sender to receiver.

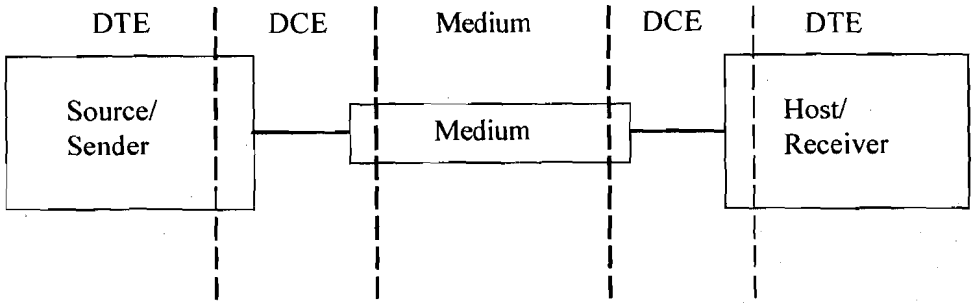

Figure 9: Data Communication-II

DCE: The interface between the Source and the Medium, and the Medium and the Receiver is called the DCE (Data Communication Equipment) (*Figure 9*) and is a physical piece of equipment.

DTE: Data Terminal Equipment is the telecommunications name given to the source and receiver's equipment. It is any device that is a source of or destination for binary digital data.

The DTE generates the data and passes them, through DCE. The DCE takes the generated data by DTE and converts them to an appropriate signal. Then this signal is introduced to telecommunication link. Most commonly used DCE is a modem, discussed in the section.

3.10 DATA FLOW

Data flow (transmission mode) is the flow of data between two points.

There are three types of dataflow *(Figure 10)*: simplex, half duplex and full duplex.

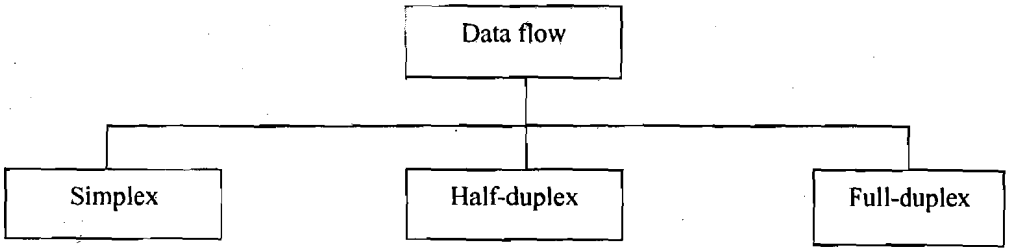

Figure 10: Data Flow

Simplex: data flows in only one direction (Figure 11) on the data communication line (medium). Examples are radio and television broadcasts. They go from the TV station to your home television.

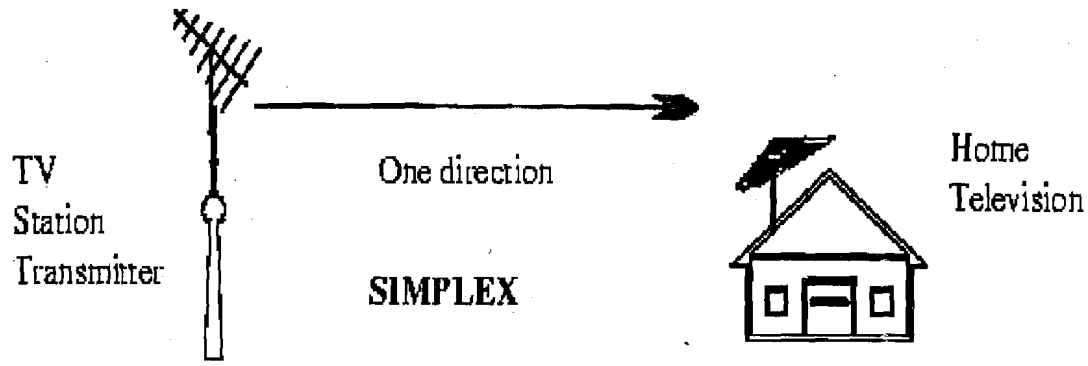

Figure 11: Simplex

Half-Duplex: Data flows in both directions but only one direction at a time (*Figure 12*) on the data communication line. Each of the stations can both transmit and receive. For example; a conversation on walkie-talkie is a half-duplex data flow. Each person takes turns talking. If both talk at once - nothing occurs!

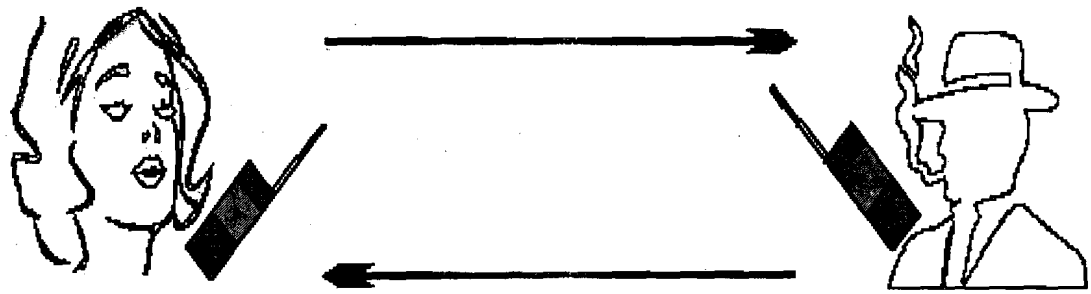

Figure 12: Half-Duplex

Bi-directional but only one direction at a time!

HALF-DUPLEX

Full-Duplex: data flows in both directions at the same time (*Figure 13*). The system is configured to flow data in both directions.

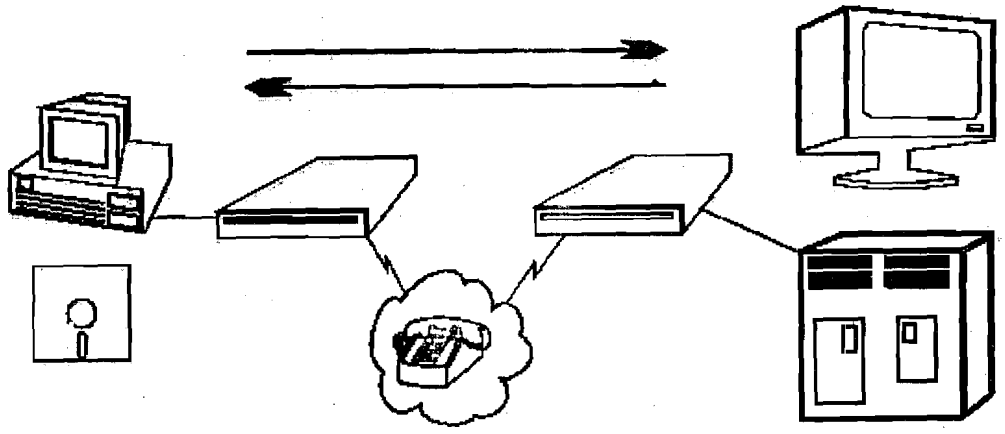

Figure 13: Full Duplex

Bi-directional both directions simultaneously!

Another example of full duplex is two-way street with traffic flowing in both directions, at the same time.

Modems

A modem (MOdulator/DEModulator) connects a terminal/computer (DTE) to the Voice Channel (dial-up line).

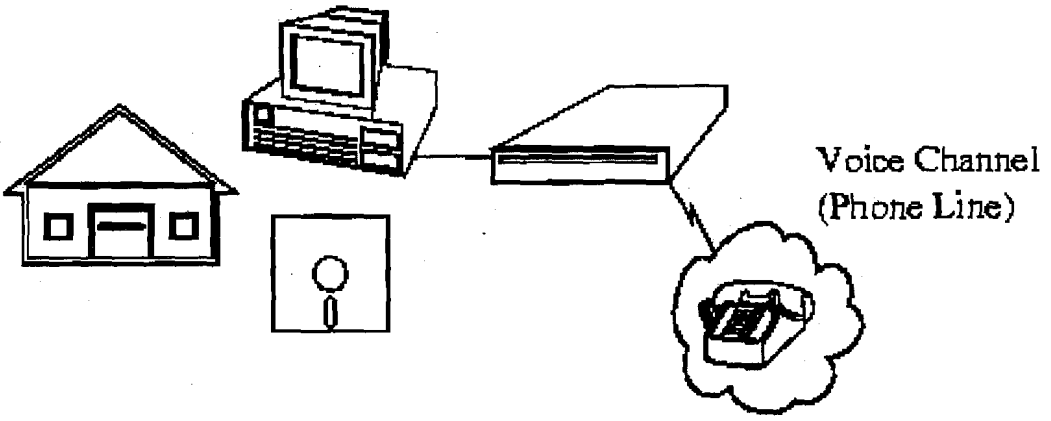

Figure 14: Modems

Basic Definition

The modem (DCE - Data Communication Equipment) is connected between the terminal/computer (DTE - Data Terminal Equipment) and the phone line (voice channel). A modem converts the DTE (Data Terminal Equipment) digital signal to an analog signal (or vice versa) that the voice channel can use.

A modem is connected to the terminal/computer's RS-232 serial port (25 pin male D connector) and the outgoing phone line with an RJ11 cable connector (the same as on a telephone extension cord). Male connectors have pins, female connectors have sockets.

Digital Connection

The connection between the modem and terminal/computer is a digital connection. A basic connection consists of a Transmit Data (TXD) line, a Receive Data (RXD) line and many hardware handshaking control lines (*Figure 15*).

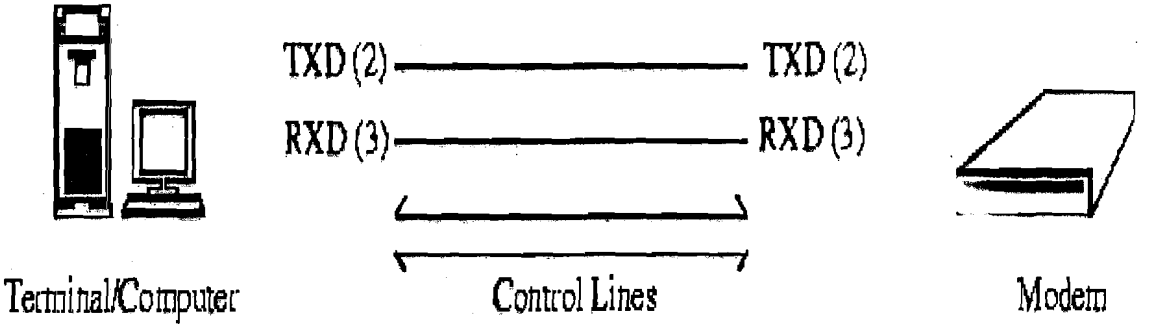

Figure 15: Digital Connection

The control lines determine whose turn it is to talk (modem or terminal), if the terminal/ computer is turned on, if the modem is turned on, if there is a connection to another modem, etc.

Analog Connection

The connection between the modem and the outside world (the phone line) is an analog connection (*Figure 16*). The voice channel has a bandwidth of 0-4 kHz but only 300 - 3400 Hz is usable for data communications.

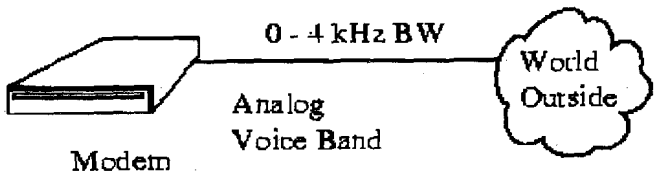

Figure 16: Analog Connection

The modem converts digital information into tones (frequencies) for transmitting through the phone lines.

External/Internal Modems

There are 2 basic physical types of modems: Internal & External modems. External modems *(Figure 17)* sit next to the computer and connect to the serial port using a straight-through serial cable.

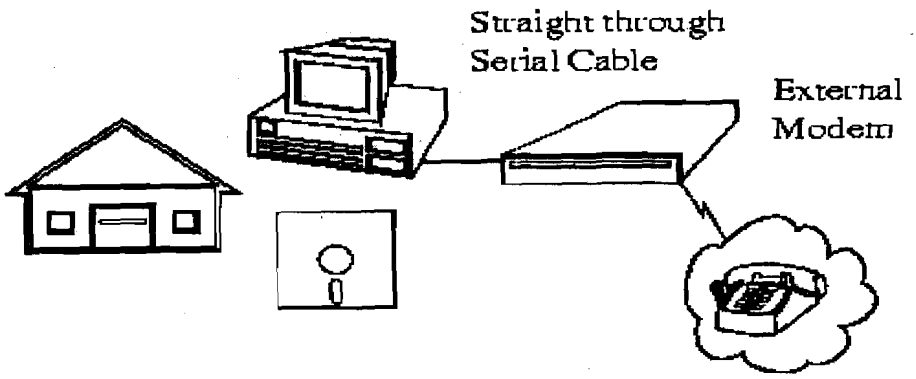

Figure 17: External Modems

Internal modems (*Figure 18*) are a plug-in circuit board that sits inside the computer. It incorporates the serial port on-board. They are less expensive than external modems because they do not require a case, power supply and serial cable. They appear to the communication programs as if they were an external modem for all practical purposes.

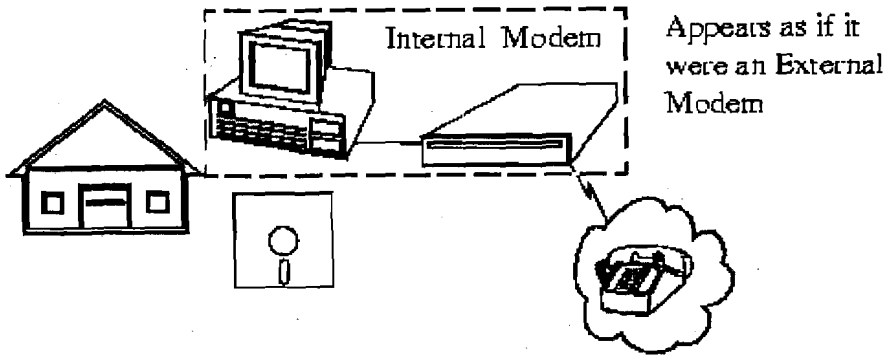

Figure 18: Internal Modems

Modem Types

There are many types of modems, the most common of which are:

(1) Optical Modem: Uses optical fiber cable instead of wire. The modem converts the digital signal to pulses of light to be transmitted over optical lines (more commonly called a media adapter or transceiver).

(2) Short Haul Modem: A modem used to transmit data over 30 km or less. Modems we use at home or to connect computers together among different offices in the same building are short haul modems.

(3) Acoustic Modem: A modem that couples to the telephone handset with what looks like suction cups that contain a speaker and microphones. Used by travelling sales people to connect to hotel phones.

(4) Smart Modem: A modem with a CPU (microprocessor) on board that uses the Hayes AT command set. This allows auto-answer & dial capability rather than manually dialing & answering.

(5) Digital Modem: Converts the RS-232 digital signals to digital signals more suitable for transmission. (Also called a media adapter or transceiver).

(6) V.32 Modem: A milestone modem that uses a 2400-baud modem with 4 bit encoding. This results in a 9600 bps (bits per second) transfer rate.

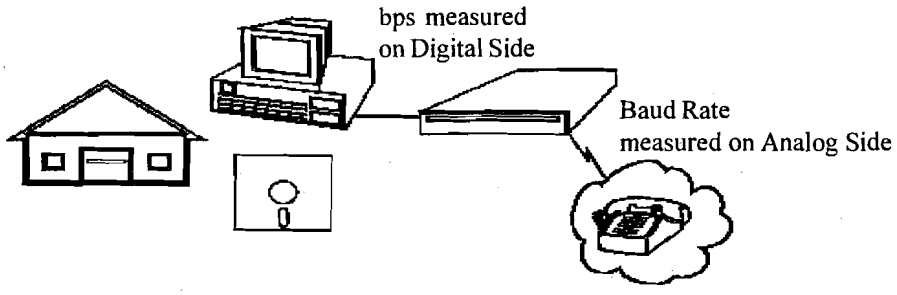

Figure 19: BPS and Baud Rate

Baud (Figure 19) is the speed at which the analog data is changing on the voice channel and bps is the speed at which the decoded digital data is being transferred.

Features of Modems

(1) Speed: The speed at which the modem can send data in bps (bits per second). Typical modem speeds are: 300, 600, 1200, 2400, 4800, 9600, 14.4K, 19.2K, 28.8K bps.

(2) Auto Dial/Re Dial: Smart modems can dial the phone number and auto re dial if a busy signal is received.

(3) Auto Answer: Most modems have Ring Detect capability and can automatically answer the telephone when an incoming call comes in.

(4) Self-Testing: Newer modems have self-testing features. They can test the digital connection to the terminal/computer and the analog connection to a remote modem. They can also check the modem's internal electronics.

(5) Voice Over Data: Voice Over Data modems allow a voice conversation to take place while data is being transmitted. This requires both the source and destination modems to have this feature.

(6) Synchronous or Asynchronous Transmission: Newer modems allow a choice of synchronous or asynchronous transmission of data. Normally, modem transmission is asynchronous (we send individual characters with just start and stop bits). Synchronous transmission or packet transmission is used in specific applications.

3.11 PHYSICAL CONNECTION

The physical connection determines how many bits (1's or 0's) can be transmitted in a single instance of time. If only 1 bit of information can be transmitted over the data transmission medium at a time then it is considered a serial communication (*Figure 20*).

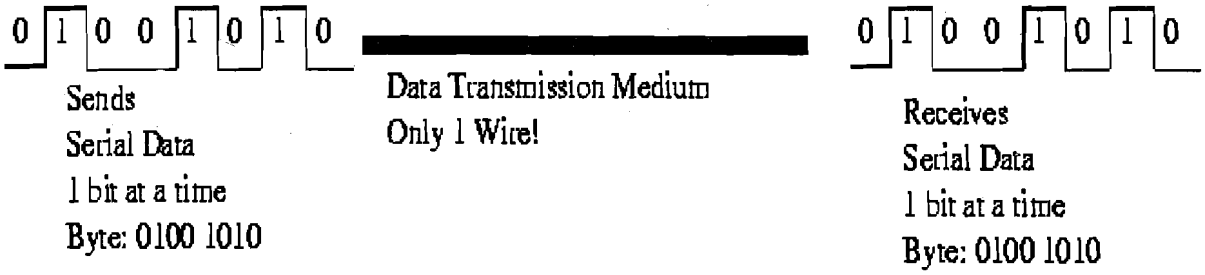

Figure 20: Serial Communication

If more than 1 bit of information is transmitted over the data transmission medium at a time then it is considered a parallel communication (*Figure 21*). By grouping, we can send data n bits at a time instead of one, through n wires.

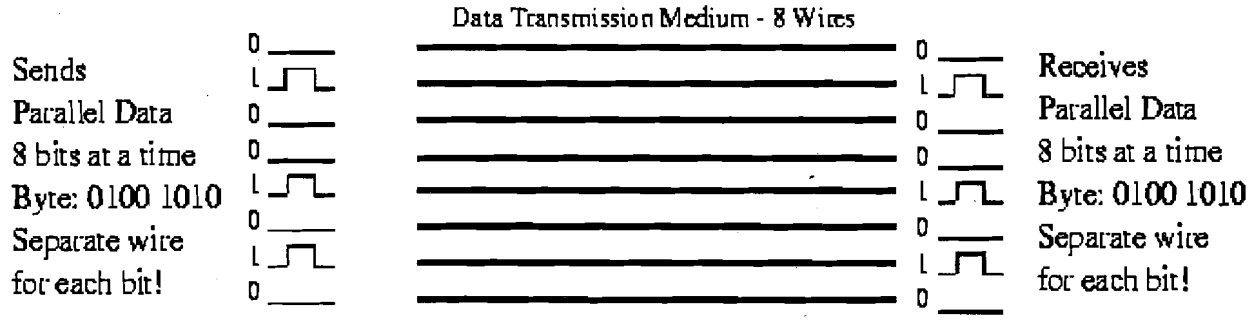

Figure 21: Parallel Communication

Communications	Advantages	Disadvantages
Parallel	Fast Transfer Rates	Short distances only More cost due to more number of lines
Serial	Long Distances	Slow transfer rates Less cost due to only one line required for serialtransmission.

3.12 TRANSMISSION MEDIA

The transmission media provide the physical path for communication among the nodes. In a computer network, where all the nodes are geometrically interconnected, it is known as its topology.

Transmission media can be broadly categorised in to two types: guided and unguided (*Figure 22).*

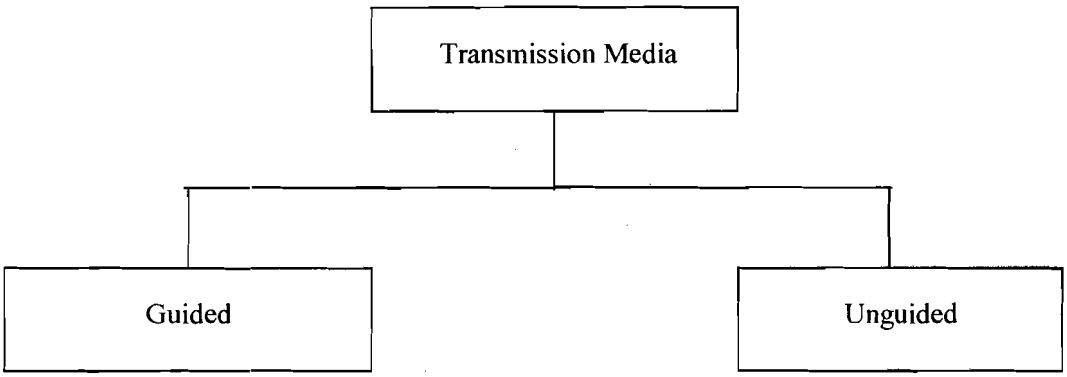

Figure 22: Type of Transmission Media

Guided transmission uses a cabling system that guides the data signals along a specific path. The data signals are bound by the cabling system. Guided media is also known as bound media. "Cabling" is meant in a generic sense, and is not meant to be interpreted as copper wire cabling only. Guided media are commonly used for point-to-point connection. The characteristics of the medium mainly decide the nature and quality of transmission. Guided media are commonly used for LAN application.

Unguided transmission media also called wireless communication consists of a means for the data signals to travel but nothing to guide them along a specific path. The data signals, not bound to a cabling media transport electromagnetic waves without using a physical conductor and are therefore often called unbound media. Unguided media are commonly used for broadcast type communication. Some examples of unguided media are sea water, free space and air. Unguided media are commonly used for WAN application.

Transmission Media Guided

There are 4 basic types of guided media:

a) Open Wire

b) Twisted Pair

c) Coaxial Cable

d) Optical Fiber

Open Wire

Open wire is (*Figure 23*) traditionally used to describe the electrical wire strung along power poles. There is a single wire strung between poles. No shielding or protection from noise interference is used. We are going to extend the traditional definition of open wire to include any data signal path without shielding or protection from noise

interference. This can include multi conductor cables or single wires. This medium is susceptible to a large degree of noise and interference and consequently is not acceptable for data transmission except for short distances of less than 20 ft.

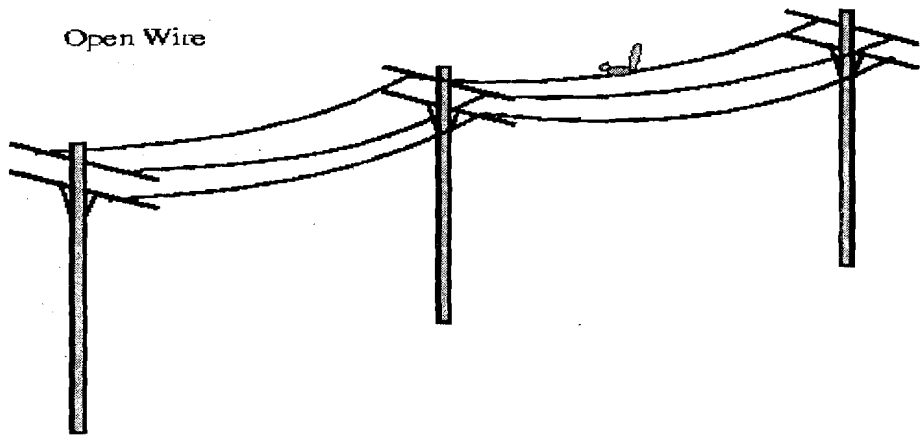

Figure 23: Open Wire

Twisted Pair

The wires in twisted pair (*Figure 24*) cabling are twisted together in pairs. Each pair consists of a wire used for the +ve data signal and a wire used for the -ve data signal. Each pair is twisted together to minimize electromagnetic interference between the pairs.Any noise that appears on 1 wire of the pair will also occur on the other wire. Because the wires are opposite polarities, they are 180 degrees out of phase (180 degrees - phasor definition of opposite polarity). When the noise appears on both wires, it cancels or nulls itself out at the receiving end.

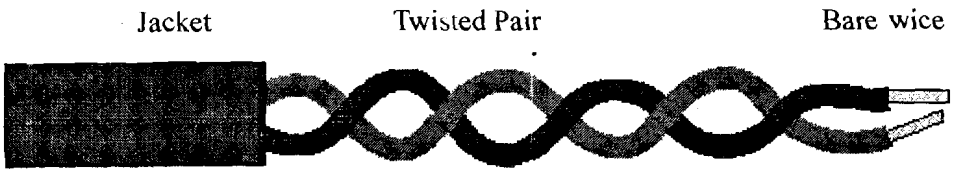

Figure 24: Unshielded Twisted Pair

The degree of reduction in noise interference is determined specifically by the number of turns per foot. Increasing the number of turns per foot reduces the noise interference. To further improve noise rejection, a foil or wire braid "shield" is woven around the twisted pairs. This shield *(Figure 25)* can be woven around individual pairs or around a multi-pair conductor (several pairs).

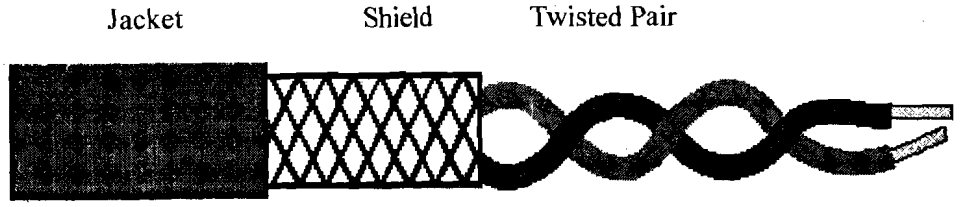

Figure 25: Shielded Twisted Pair

Shielded Twisted Pair

The twisted pair can be shielded (*Figure 25*) with metallic braid, to reduce the interference Cables with a shield are called shielded twisted pair and are commonly abbreviated STP. Cables without a shield are called unshielded twisted pair or UTP. Twisting the wires together results in characteristic impedance for the cable. Typical impedance for UTP is 100 ohm for Ethernet 10BaseT cable.

UTP or unshielded twisted pair cable is used on Ethernet 10BaseT and can also be used with Token Ring. It uses the RJ line of connectors (RJ45, RJ11, etc.)

Use Twisted pair can be used for both analog and digital communication. Twisted pair cables are most effectively used in systems that use a balanced line method of transmission: polar line coding (Manchester Encoding) as opposed to unipolar line coding (TTL logic). Most popular use of twisted pair is in our oldest telephone system. It is also used in LAN for point-to point short distance communication

Coaxial Cable

Coaxial cable (*Figure 26*) consists of two conductors. The inner conductor is held inside an insulator with the other conductor woven around it providing a shield. An insulating protective coating called a jacket covers the outer conductor.

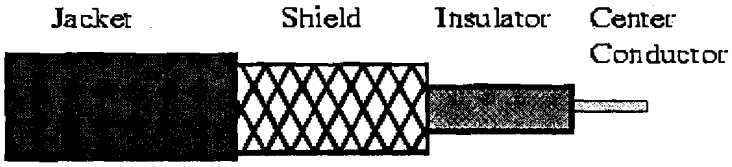

Figure 26: Coaxial Cable

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. Typical impedances for coaxial cables are 75 ohms for Cable TV, 50 ohms for Ethernet Thinnet and Thicknet. The excellent control of the impedance characteristics of the cable allow higher data rates to be transferred than with twisted pair cable.

Optical fiber

Optical fiber consists of thin glass fibers that can carry information at frequencies in the visible light spectrum and beyond. The typical optical fiber consists of a very narrow strand of glass called the core. Around the core is a concentric layer of glass called the cladding. A typical core diameter is 62.5 microns (1 micron = 10^{-6} meters). Typically Cladding has a diameter of 125 microns. Coating the cladding is a protective coating consisting of plastic, it is called the Jacket.

Optical fibers work on the principle that the core refracts the light and the cladding reflects the light. The core refracts the light and guides the light along its path. The cladding reflects any light back into the core and stops light from escaping through it - it bounds the medium.

Advantages of Optical Fiber

- Noise immunity: RFI and EMI immune (RFI - Radio Frequency Interference, EMI -Electromagnetic Interference) because fiber –optic transmission uses light rather than electricity, noise is not a factor.
- Security: cannot tap into cable.

- Large Capacity due to BW (bandwidth).
- No corrosion.
- Longer distances than copper wire.
- Smaller and lighter than copper wire.
- Faster transmission rate.

Disadvantages of optical fiber

- Physical vibration will show up as signal noise!
- Limited physical arc of cable. Bend it too much and it will break!
- Difficult to splice.

The cost of optical fiber is a trade-off between capacity and cost. At higher transmission capacity, it is cheaper than copper. At lower transmission capacity, it is more expensive.

Infrared

Infrared (IR) transmission is another line of sight medium .Infrared technology uses electromagnetic radiation of wave lengths between radio waves and visible light, operation between 100GHZ and 100THZ (terahertz). These frequencies are very high offering nice data transfer rates. We are used to seeing infrared technology utilised for our television or VCR remotes. IR is generally restricted to LAN within or between buildings

Advantages

1) Higher bandwidth means superior throughput to radio
2) Inexpensive to produce
3) No longer limited to tight interroom line-of-sight restrictions

Disadvantage

1) Limited in distance
2) Cannot penetrate physical barriers like walls, ceilings, floors, etc.

3.13 CONNECTING DEVICES

As companies grow, so do their networks. When a network outgrows its original design, the network becomes slow and print jobs take longer to be completed. In such cases it is a better idea to segment the existing LAN so that each segment becomes a separated LAN.

We can connect two or more networks together to create larger networks. A LAN (local area network) can be connected to another LAN. A LAN (local area network) can be connected to another WAN (wide area network). The components or devices that are employed to connect two or more networks together are:

1) Repeaters
2) Hubs
3) Bridges
4) Routers
5) Gateways

3.13.1 Repeaters

Repeaters, also called regenerator, are physical hardware devices. They connect two network segments and broadcast packets between them, thus extending your network beyond the maximum length of your cable segment. They have the primary function to regenerate the electrical signal (shown below):

- Reshaping the waveform
- Amplifying the waveform
- Retiming the signal, to avoid collision on the network

As signal travels along a cable, its strength or amplitude decreases. This is called attenuation. In other words, the signal attenuates as it travels along a cable. This limits the length of a cable used to connect the computers together.

Since signal is a factor in the maximum length of a segment, repeater can regenerate (or amplify) the weak signals so that they can travel additional cable lengths. A repeater has intelligence ,so that it takes a weak signal from one cable segment, regenerates it and passes it on to the next segment. Simply we can say that it recreates the bit pattern of the original signal . No more than four repeaters are used to join segments together to keep collision detection working properly. We should not confuse repeater with amplifiers. As the amplifier uses analog signal, it cannot differentiate between original signal and noise, therefore it amplifies both original signal and noise. The repeater does not amplify the original signal, it regenerates the original bit pattern.

Purpose of a Repeater

The purpose of a repeater (Figure 27) is to extend the LAN Segment beyond its physical limits (as defined by the Physical Layer's Standards: e.g. Ethernet is 500m for 10Base5). A LAN Segment is a logical path, such as the logical bus used by all 802.3 Ethernet types. A LAN Segment is given an identification number, called a Segment Number or Network Number, to differentiate it from other segments.

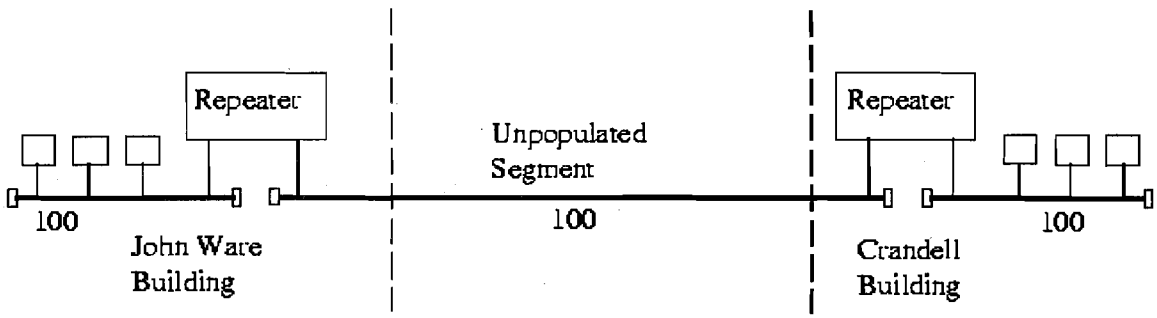

Figure 27: Repeater

Typically, repeaters are used to connect two physically close buildings together (when they are too far apart to just extend the segment). They can be used to connect floors of a building that would normally surpass the maximum allowable segment length. Note: for large extensions, as in the above example, two Repeaters are required. For shorter extensions, only one Repeater may be required.

Repeater's OSI Operating Layer

Repeaters operate at the OSI Model Physical Layer (*Figure 28*).

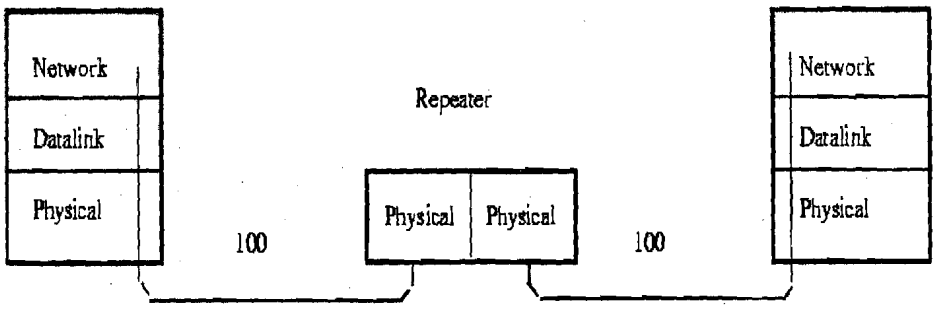

Figure 28: Repeater's Segment-to-Segment Characteristics

A repeater cannot join two cable segments using different access methods. A repeater is not used to connect a segment using CSMA/CD access method to a segment using token passing access. Repeaters can join two different physical media, but they must use the same access method. Thus a repeater can have physical connections to join a coaxial cables segment to a fiber optic segment.

Repeaters do not "de-segment" a network. All traffic that appears on one side of the repeater appears on both sides. Repeaters handle only the electrical and physical characteristics of the signal.

Repeaters work only on the same type of Physical Layer: Ethernet-to-Ethernet, or Token Ring-to-Token Ring. They can connect 10Base5 to 10BaseT because they both use the same 802.3 MAC layer.

You can run into problems with the transfer rate (1 Mbps vs. 10 Mbps) when you connect 1Base5 to 10BaseT. A repeater cannot connect Token Ring to Ethernet because the Physical Layer is different for each network topology.

Repeater Addressing: MAC Layer and Network Segment

The MAC Layer Address is used to identify the Network Card to the Network. The Repeater is transparent to both sides of the segment and both sides can "see" all the Mac Addresses (regardless of which side they are on). This means that any network traffic on Floor 1 will also appear on Floor 5, and vice versa (*Figure 29*).

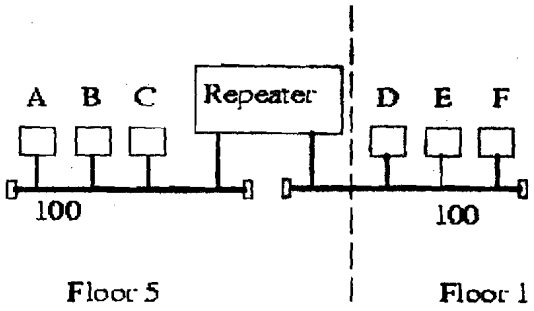

Figure 29: Repeater Addressing

Nodes A & B could be furiously are exchanging files; this network traffic would also appear on Floor 1. Repeaters don't provide isolation between segments (there is only one collision domain).

Because Repeaters provide no isolation between segments, and the repeater is transparent to both sides of the segment, both sides of the repeater appear as one long segment. The Network Number, or Segment Number, is the same on both sides of the Repeater.

3.13.2 Hubs

Hubs can also be called either Multi port Repeaters or Concentrators. They expand one Ethernet connection into many. They are physical hardware devices. A hub is

similar to a repeater, except that it broadcasts data received by any port to all other ports on the hub.

Some hubs are basic hubs with minimum intelligence (i.e. no microprocessors), Intelligent Hubs can perform basic diagnostics, and test the nodes to see if they are operating correctly. If they are not, the Smart Hubs (or Intelligent Hubs) will remove the node from the network. Some Smart Hubs can be polled and managed remotely.

Purpose of Hubs

Hubs are used to provide a Physical Star Topology (*Figure 30*). The Logical Topology is dependent on the Medium Access Control Protocol. At the center of the star is the Hub, with the network nodes located on the tips of the star.

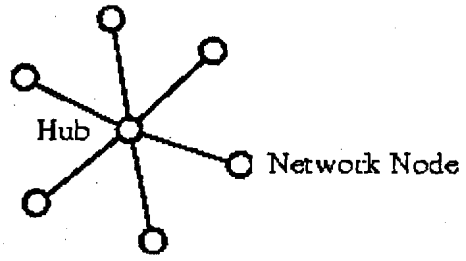

Figure 30: Position of Hub

Star Topology

The Hub is installed in a central wiring closet (Figure 31) with all the cables extending out to the network nodes. The advantage of having a central wiring location is that it is easier to maintain and troubleshoot large networks. All of the network cables come to the central hub. This way, it is especially easy to detect and fix cable problems. You can easily move a workstation in—a star topology— by changing the connection to the hub at the central wiring closet.

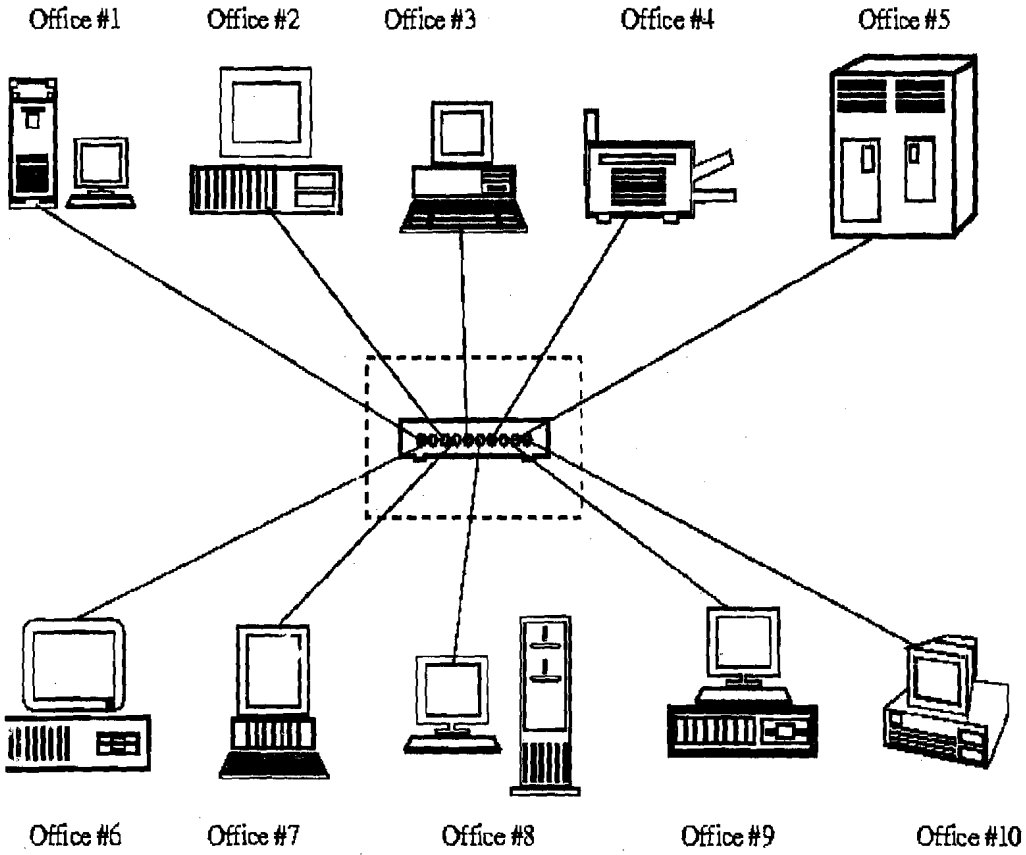

Figure 31: Example of Hub

Hub's OSI Operating Layer

Hubs are multi port repeaters, and as such they obey the same rules as repeaters (See previous section OSI Operating Layer). They operate at the OSI Model Physical Layer.

Hub's Segment-to-Segment Characteristics

To understand the Ethernet segment-to-segment *(Figure 32)* characteristics of a hub, determine how the Ethernet Hubs operate. Logically, they appear as a Bus Topology, and physically as a Star Topology. Looking inside an Ethernet Hub, we can see that it consists of an electronic printed circuit board (which doesn't tell us much). If we form a functional drawing, then we can clearly see how the Physical and Star Topology appears:

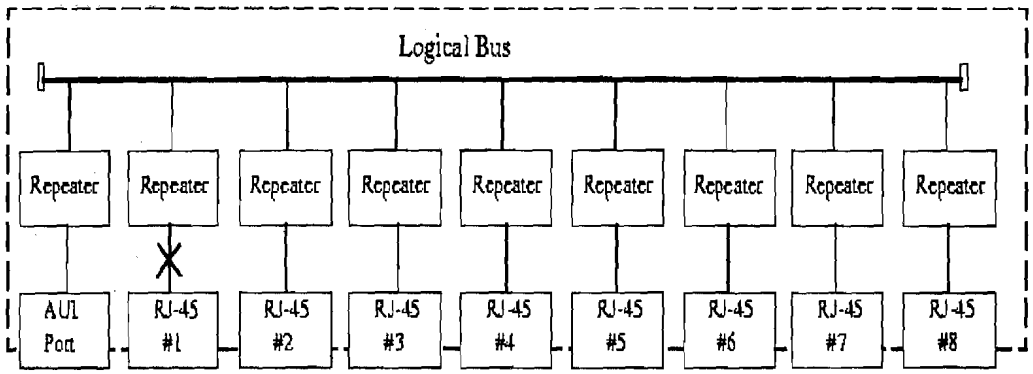

Figure 32: Hub's Segment to Segment

Understanding that inside the Hub is only more repeaters, we can draw the conclusion that all connections attached to a Hub are on the same Segment (and have the same Segment Number). A single repeater is said to exist from any port to any port, even though it is indicated as a path of 2 repeaters.

Hub's Addressing

Again, because a Hub is just many repeaters in the same box, any network traffic between nodes is heard over the complete network. As far as the stations are concerned, they are connected on one long logical bus (wire).

Switching Hubs

Switching hubs (*Figure 33*) are hubs that will directly switch ports to each other. They are similar to full duplex hubs, except that they allow dedicated 10 Mbps channels between ports.

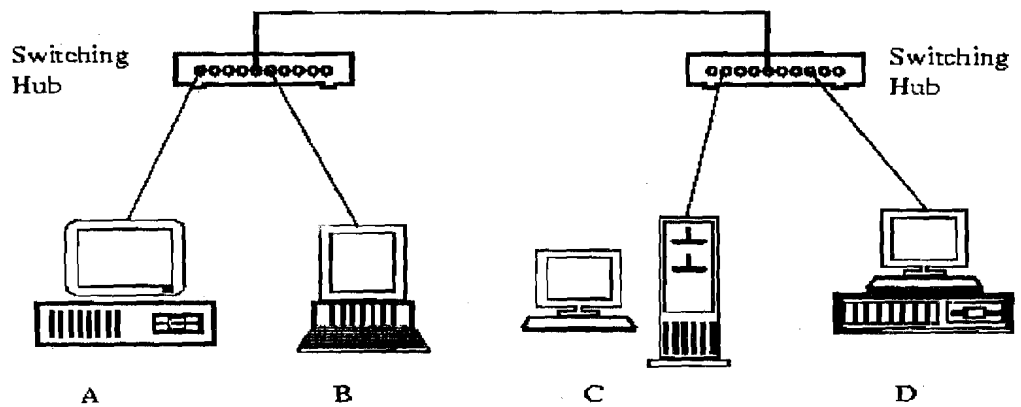

Figure 33: Switching Hub

If A wanted to communicate with B, a dedicated 10 Mbps connection would be established between the two. If C wanted to communicate with D, another dedicated 10 Mbps connection would be established.

3.13.3 Bridges

Bridges have all the features of the repeater. Besides regenerating the signals, a bridge can segment (or divide) a network to isolate traffic related problems. A bridge sends the data frames only to the concerned segment, thus preventing excess traffic. A bridge can split an overloaded network into two separate networks, reducing the amount of traffic on each segment and thus making each network more efficient. Just like repeaters, the bridges can be used to link different physical media. Bridges can also be used to connect dissimilar networks like Ethernet system to a Token Ring system. Thus bridges can be used to join networks using CSMA/CD access and token passing access.

Bridges are both hardware and software devices. They can be standalone devices — separate boxes specifically designed for bridging applications— or they can be dedicated PCs (with 2 NICs and bridging software). Most server software will automatically act as a bridge when a second NIC card is installed.

Bridge OSI Operating Layer

Bridges (*Figure 34*) operate on the OSI Model Data Link Layer, while repeaters work at the physical layer. Since bridges work on a higher layer than repeaters, they are more complex than repeaters and cost more than repeaters. They look at the MAC addresses for Ethernet and Token Ring, and determine whether or not to forward--or ignore—a packet.

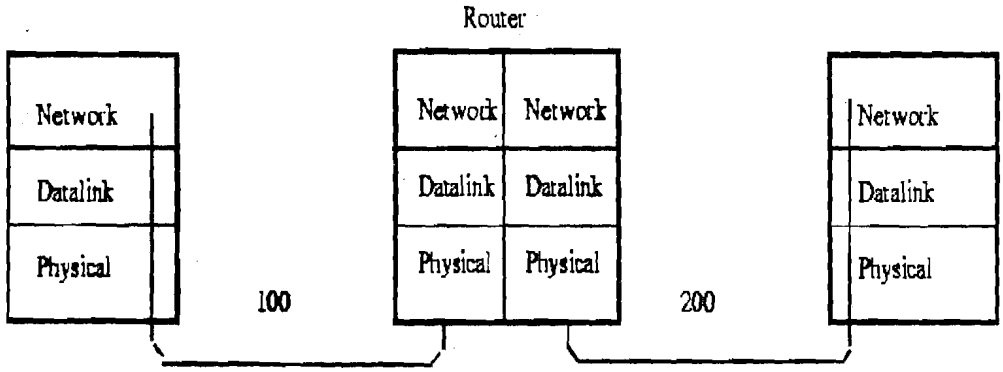

Figure 34: Bridge OSI Operating Layer

Bridges have their own routing tables. Initially the bridge's routing table is empty. As nodes send packets, the source address is copied to the routing table. With this address information, the bridge learns where the computers are situated. When any packet is received by a bridge it reads its source and destination address. If the bridge knows the location of the destination node it forwards the packet to the segment on which the destination node is situated. If it does not know the destination, it forwards the packet to all the segments.

Purposes of a Bridge

The purposes of a Bridge are the following:

- Isolates networks by MAC addresses
- Manages network traffic by filtering packets
- Translates from one protocol to another

Isolates networks by MAC addresses

For example, you have one segment called Segment 100: it has 50 users (in several departments) using this network segment. The Engineering Dept. is CAD (Computer Aided Design) -oriented, while the Accounting Dept. is into heavy number crunching (year end reports, month end statements, etc.).

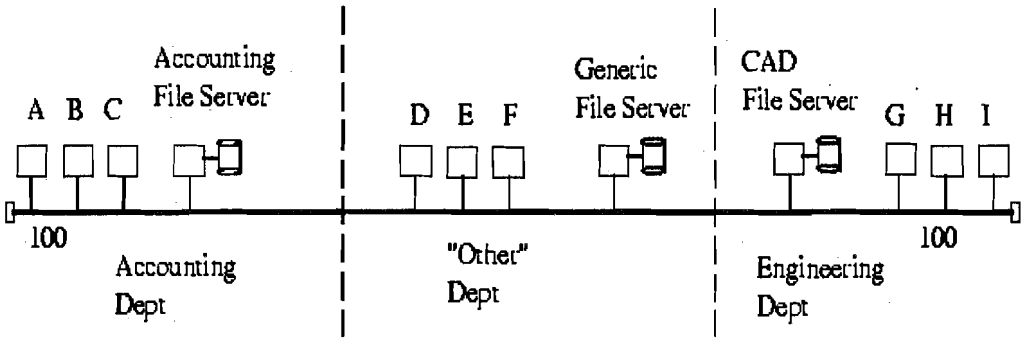

Figure 35: Bridge Example 1

On this network, any traffic between Clients A, B or C and the Accounting File Server (in the Accounting Dept.) will be heard across the Segment 100. Likewise, any traffic between the Engineering Dept. Clients G, H or I (to the CAD File Server) will be heard throughout the Network Segment. The result is that "Other" Department accesses to the Generic File Server are incredibly slow: this is because of the unnecessary traffic that is being generated from other departments (Engineering & Accounting).

The solution is to use one Bridge (*Figure 36) to* isolate the Accounting Dept., and another bridge to isolate the Engineering Department. The Bridges will only allow packets to pass through that are not on the local segment. The bridge will first check its "routing" table to see if the packet is on the local segment. If it is, it will ignore the packet, and not forward it to the remote segment. If Client A sent a packet to the Accounting File Server then Bridge #1 will check its routing table (to see if the Accounting File Server is on the local port). If it is on the local port, then Bridge #1 will not forward the packet to the other segments.

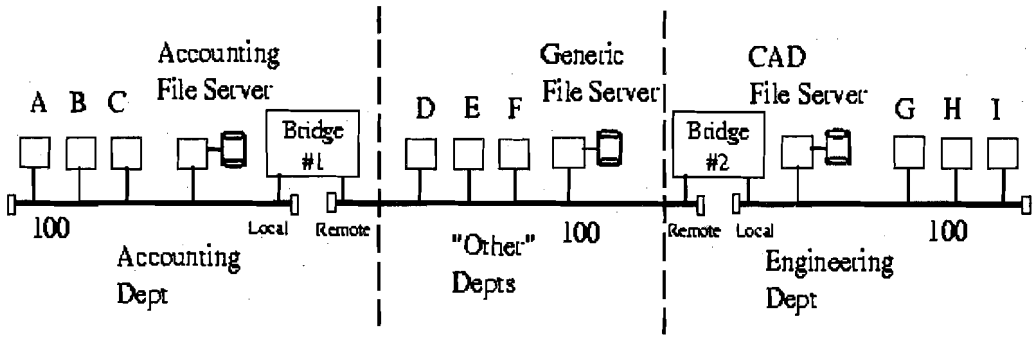

Figure 36: Bridge Example 2

If Client A sent a packet to the Generic File Server, Bridge #1 will again check its routing table to see if the Generic File Server is on the local port. If it is not, then Bridge #1 will forward the packet to the remote port.

Note: The terms local and remote ports are arbitrarily chosen to distinguish between the two network ports available on a bridge.

In this manner, the network is segmented, and the local department traffic is isolated from the rest of the network. Overall network bandwidth increases because the Accounting Dept. does not have to fight with the Engineering Dept. (for access to the segment). Each segment has reduced the amount of traffic on it and the result is faster access. Each department still has complete access to the other segments, but only when required.

3.13.4 Routers

A router is a special –purpose computer having a processor (CPU) and memory like any other computer. But unlike any other computer, it has more than one I/O interface that allows it to connect to multiple computer networks.

Routers are both hardware and software devices. Just like bridges, Router can connect network segments and filter and isolate traffic. Unlike a bridge, a router can connect networks that use different technologies, addressing methods, media types, frame formats, and speeds. Routers are used in complex network situations because they provide better traffic management than bridges. A router keeps track of the address of all the segment of a network and can even determine the best path for sending data. Routers do not pass broadcast traffic.

Like bridges, the routers also maintain routing tables in their memories to store information about physical connections on the network. The router examines each packet of data, checks the routing table , and then forwards the packet if necessary. Routers are more inelegant than bridges, as routers can share status and routing information with one another and use this information to bypass slow or malfunctioning connections. Routers do not maintain any state information about the packets; they simply move them along the network. Routers are usually employed by wide area networks using dissimilar addressing schemes and different communication protocols.

Routers do not allow bad data to get passed on to the network. Thus they save networks from broadcast storms.

There are two types of routers – static routers and dynamic routers.

Static routers require an administrator to manually set up and configure the routing table and to specify each route.

Dynamic routers maintain a routing table automatically and require minimal set up and configuration.

Router OSI Operating Layer

Routers operate on the OSI Model's Network Layer as shown in *Figure 37*. The Internet work must use the same Network Layer protocol. Routers allow the transportation of the Network Layer PDU through the Internetwork, even though the Physical and Data Link Frame size and addressing scheme may change.

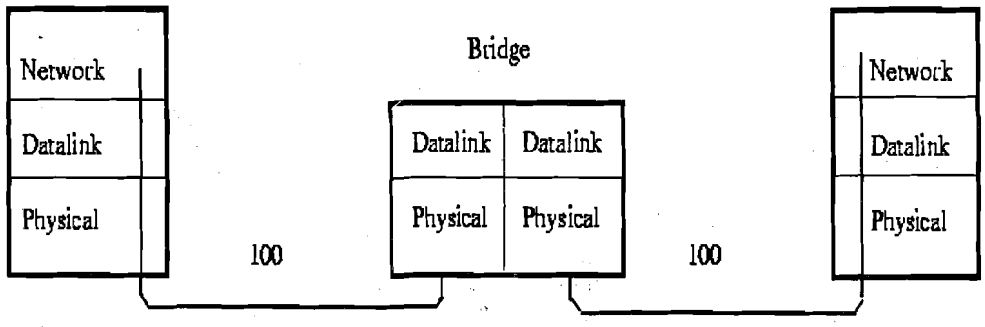

Figure 37: Router Segment-to-Segment Characteristics

Routers that only know Novell IPX (Internetwork Packet Exchange) will not forward Unix's IP (Internetwork Packet) PDUs, and vice versa. Routers only see the Network Layer protocol that they have been configured for. This means that a network can have multiple protocols running on it (e.g. SPX/IPX, TCP/IP, Appletalk, XNS, etc.).

Router Addressing

Routers know the address of all known networks. They maintain a table of pathways between networks and can select an optimal route over which to send data. Routers look only at network address and not at destination node address. Routers talk to other routers, but not to remote computers.

Routers combine the Network Number and the Node Address to make Source and Destination addresses (in routing Network Layer PDUs across a network). Routers have to know the name of the segment that they are on, and the segment name or number where the PDU is going. They also have to know the Node Address: MAC Address for Novell, and the IP address for TCP/IP.

3.13.5 Gateways

A Gateway is the Hardware/Software device that is used to interconnect LANs & WANs

Gateways are much more complex and powerful than a router. They are slower than a router and are expensive. A Gateway incorporates the functions of routers and bridges, but it can translate instruction set on sending network into corresponding instruction set of the receiving network. Gateways make communication possible between different architectures and environments.

Often, the router that is used to connect a LAN to the Internet will be called a gateway. It will have added capability to direct and filter higher layer protocols (layer 4 and up) to specific devices (such as Web servers, ftp servers and e-mail servers).

A Gateway links two systems that do not use the same communication protocols, data formatting structures, languages and architecture, which can not be done by a router. Gateways perform protocol and data conversion.

Gateway's OSI Operating Layer

A Gateway operates at the Transport Layer and above and it typically translates each source layer protocol into the appropriate destination layer protocol. Gateways use all the seven layers of the OSI model A mainframe gateway may translate all OSI Model layers. For example, IBM's SNA (System Network Architecture) does not readily conform to the OSI Model, and requires a gateway to translate between the two architectures.

☞ Check Your Progress 1

1) Compare the advantage of fiber over copper wire.

.....

.....

2) Discuss the advantages and disadvantages of Bus & Mesh Topologies.

.....

.....

3) What are the roles of protocols in a computer network?

.....

.....

3.14 SUMMARY

- A network allows one to share access to information devices.
- Communication protocol is a set of conventions or rules that must be adhered to by both communicating parties to ensure that information being exchanged between the two parties is received and interpreted correctly.
- The major criteria to judge a data communication network are: performance Consistency, Reliability, Recovery, Security.
- The topology is the geometric arrangement (either physically or logically) of the linking devices (usually called nodes) and the links, connecting the individual computers or nodes together. Different topologies are mesh, star, ring or combined topology.
- Communication between two devices can occur in three transmission modes: simplex, half-duplex or full duplex.
- Computer network is classified into three types: LAN, MAN and WAN.
- The network of networks is called the Internet.
- The most familiar type of DCE is the modem that modulates and demodulates signals.
- Guided transmission media use a cabling system that guides the data signals along a specific path.
- Unguided transmission media consist of a means for the data signals to travel but nothing to guide them along a specific path.
- Repeater is a device that operates at the physical layer, bridge at the data link layer, router at the network layer and Gateway at all seven layers of the OSI model.

3.15 SOLUTIONS/ANSWERS

Check Your Progress 1

- Noise immunity: RFI and EMI immune (RFI - Radio Frequency Interference, EMI -Electromagnetic Interference) Because fiber –optic transmission uses light rather than electricity, noise is not a factor.
- Security: cannot tap into cable.
- Large Capacity due to BW (bandwidth).
- No corrosion.
- Longer distances than copper wire.
- Smaller and lighter than copper wire.
- Faster transmission rate.

The cost of optical fiber is a trade-off between capacity and cost. At higher transmission capacity, it is cheaper than copper. At lower transmission capacity, it is more expensive.

2) **The Bus Topology**

The main advantage of bus topology is that it is quite easy to set up. Any workstation can be easily moved to another location as bus runs throughout the office. Another benefit of this layout is that if one computer on the bus fails, it does not affect the rest of the traffic on the bus.

A network with bus topoiogy cannot become too big as all the traffic is on a single bus. The entire network can be down only if the bus has a break. The open ends of the bus must be terminated to prevent signal bounce. If one or both ends of the bus are not terminated, the whole network can be down.

Disadvantages include difficult reconfiguration and fault isolation

Mesh Topologies

In a mesh topology, every node has a dedicated point-to point link to every other node. Simply dedicated means that the links carry traffic only between the two nodes. So mesh topology does not have traffic congestion problems. Every node has n-1 link, for a fully connected mesh topology having n nodes. So total number of links will be n (n-1).This also means that every node has (n-1) I/O ports

Advantages of Mesh topology

1) Use of dedicated links guarantees that each connection can carry its own data load. This eliminates the traffic problem.

2) If one link fails, it does not affect the rest of network. This means it is robust.

3) Point to point links make fault identification and fault isolation easy.

4) Privacy or security is high; as any other link cannot gain access to dedicated link where the message is travailing.

Disadvantages of mesh topology

1) More cabling and I/O ports are required, because every node must be connected to every other node.

2) Cost is very high, because more number of nodes and cabling required.

3) Installation and reconfiguration is difficult.

4) The complexity of writing communication software can be reduced by adopting the principle of protocol layering. The idea here is to partition communication functions into a vertical set of layers. Each layer performs a related set of functions. Division of work between layers is done in such a way that they are manageable and provide a logical interface and break point. Each communication layer provides certain services to layers above it and relies on the next lower layer to perform more primitive functions. Each layer hides internal details from other layers. Thus dividing the communication problem into several layers reduces its complexity and makes the work of developing communication software a lot easier and error free.

3.16 FURTHER READINGS

1) *"Computer Networks, Tanenbaum"*, Third Edition, Prentice-Hall 1996.

2) *"Data and Computer Communications"*, William Stallings, Fourth Edition, MacMillan, 1994.

3) *"Data communication and networkings"*. Behrouz A.Forouzan 2nd edition, TMH 2000.

4) *"Internetworking with TCP/IP", Douglas Comer,* Volume I, Fourth Edition, Prentice Hall, 2000.