Chapter 1

Introduction to Computer Networking

1.0 OBJECTIVES

After studying this chapter you will be able to-

- ✓ Explain computer networks.
- ✓ Discuss the need of network in today's world.
- ✓ State the advantages of network.
- ✓ Discribe Client Server Model.
- ✓ Explain Different types of networks.

1.1 INTRODUCTION

Each of the past three centuries has been dominated by a single technology. People were doing lot of paper work in organizations because, lack of advance systems which will help them in their day today work. The 18th century was the time of the great mechanical systems accompanying the Industrial revolution. Computer industry has made spectacular progress in short time. During the first two decades of their existence. Computer systems were highly centralized, usually within the single large room. A medium size company or university might have had one or two computers, white large institutions had at most few dozen. The idea that within 20 years equally powerful computers smaller than postage stamps would be mass-produced by the millions was pure science fiction.

The merging of computers and communications has had a profound influence on the way computer systems are organized. The old model of single computer serving all of the organization computational need has been replaced by one which the-large no of separate but interconnected computers do the fob. These systems are called has computer network.

A network is a group of two of more computer systems sharing services and interacting in some manner. This interaction is, accomplished through a shared communication link, with the shared components being data. Put simply a network is a

collection of machines have been linked both physically and through software components to facilitate communication and the sharing of information.

A physical pathway known as transmission medium, connects the systems and a set of rules determines how they communicate. These rules are known as protocols. A network protocol is software installed on a machine that determines the agreed –upon set of rules for two or more machine to communicate with each other. One common metaphor used to describe different protocols is to compare them to human languages.

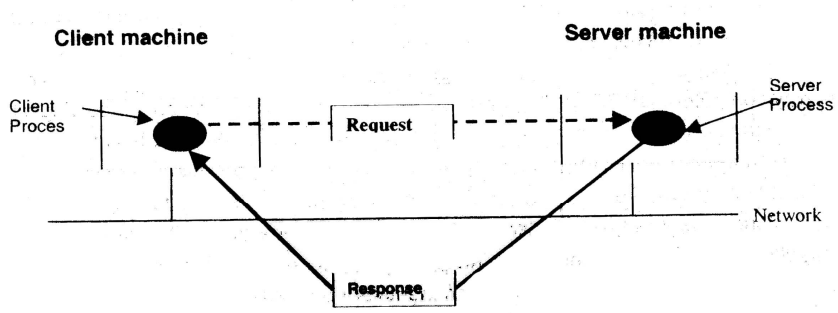
Think of a group of people in the same room who know nothing about each other. In order for them to communicate, this group must determine what language to speak, how to handle identifying each other, whether to make general announcements or have private conversations and so on. Machines using different protocols installed can't communicate with each other.

Networks are widely used by companies or on personal level also. Network for companies should provide high reliability, cost efficient, and recourse sharing.

1.2 CLIENT SERVER MODEL

Normally network should provide high reliability; emergency back up etc. For satisfying this purpose big mainframe computers are required. But this will be not cost efficient. On other side small computers have a much better price/performance ratio than the large Ones. Mainframes (room-Size) computers are roughly a factor of ten faster than personal computers, but they cost thousand times more. This imbalance has cost many system designers to build systems consisting of personal computers, one per user with data kept on one or more shared file server machines.

In this model the users are called clients, and the whole arrangement is called as Client-Server model, (as shown below)



In the client server model communication generally takes the form of a request Message from the client to server asking for some work to be done. The server then does the work and sends back the reply. Usually there are many clients using a small no. of servers.

Check Your Progress -1.2

1) Answer in 1-2 sentences.

a. What is Network?

……

……

b. What is Protocol?

……

……

c. Define Client

……

……

d. Define Server

……

……

2) Fill in the blanks.

1. A Network is a group of two or more computer system sharing …….
2. In client server model users are called as ……..

3) Match the following

1. Network	a. Response
2. Client	b. Group of computers
3. Server	c. Request

1.3 TYPES OF NETWORK

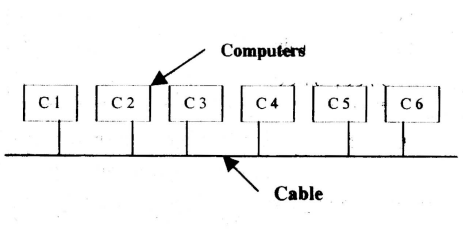
The network can be divided into geographical areas and fall into one of two major categories

- Local Area Network (LANs)
- Metropolitan Area Network (MANs)
- Wide Area Network (WANs)
- Wireless Networks

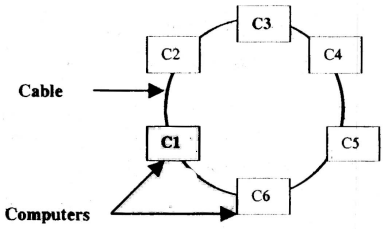
1.3.1 Local Area Network

A LAN is generally confined to a specific location, such as floor, building or some other small area. By being confined it is possible in most cases to use only one transmission medium (cabling). The technology is less expensive to implement than WAN because you are keeping all of your expenses to a small area, and generally you can obtain higher speed. They, are widely used to connect personal computers and workstations in company offices and factories to share recourses.

LANs often use a transmission all the machines are attached with each other. Traditional LANs runs at speed of 10 to 100 mbps have low delay and make very few errors. Never LANs may operate at higher speed up to 100 megabytes/sec.



LAN with Bus Topology



LAN with ring topology

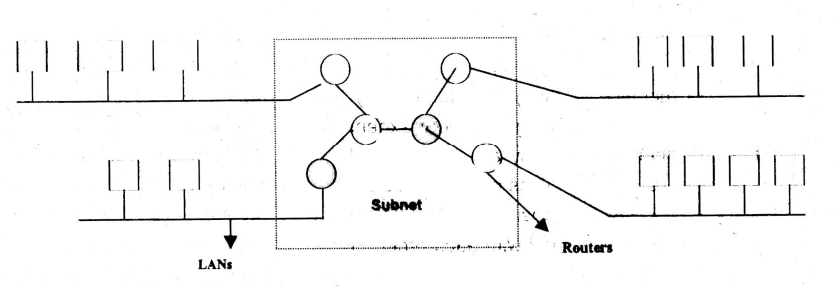
1.3.2 Metropolitan Area Network (Man)

Metropolitan Area Network is basically a bigger version of LAN and normally uses same technology. It might cover a group of nearby corporate offices or a city and might be either private or public. On other hand, MAN is network running through out a metropolitan are such as a backbone for a phone service carrier. A MAN just has one or two cables and does not contain switching elements.

1.3.3 Wide Area Network (WAN)

A wide area network spans a large geographical area, often a country or continent. It multiplies multiple connected LANs; that can be separated by any geographical distance. A LAN at the corporate headquarters in Indianapolis can be connected to a LAN at field office in Chicago and to another field office LAN in St. Louis to form a single Wide Area Network.

In most WANs the network contains numerous cables or telephone lines, each one connection a pair of routers. If two routers that do not share a cable nevertheless and wish to communicate, they must do it indirectly. On personal computers we are using modem to communicate indirectly with other computer.



1.3.4 Wireless Networks

Mobile computers such as notebook computers laptops are fastest growing segment of computer industry. Users wants to connect this machine to their office LANs to see the data when they .are out from the office, since the wired connection is not possible we have to use wireless networks.

For e.g. on Aircraft single router will maintain a radio link with some other router on ground, changing routers as it flies along this configuration is just a traditional LAN, except that its connection to the outside world happens to be a radio link instead of a hardwired line.

1.3.5 Internet works

Many networks exist in world, often with different hardware and software. People connected to one network .always want to communicate with, people attached to a different one. This requires connecting together different, and frequently incompatible networks, sometimes by using machines called as gateways to make the connection and provide the necessary translation, both in terms of hardware and software. Such collection of interconnected networks is called as Internet works or Internet.

A common form of Internet is collections of LANs connected by WA are form when distinct networks are connected with each other through routers and hosts.

Check Your Progress 1.3

1) Answer in brief.

a. List different types of networks?

……

……

b. Explain Local area network?

……

……

c. Explain Wide area network?

……..……..……

……..……..……

2) File in the blanks

1. LAN run at speed of …….. Mbps
2. …… is basically a bigger version of LAN
3. Internetworks are form when no. of network connected through ……..…… and ……..

3) Match the following

1.	MAN	a. Wide Area Network
2.	LAN	b. Metropolitan area network
3.	WAN	c. 10 to 100 Mbps

1.4 SUMMARY

In this chapter we have studied the old model of single computer serving all of the organization's computational need has been replaced by one in which the large no of separate but interconnected computers do the job. These systems are called as computer network. A network is a group of two or more computer systems sharing services and interacting in some manner.

In the end Computer network are mainly divided into Local Area Network**,** Metropolitan area network, wide area network, wireless networks, Internetworks.

1.5 CHECK YOUR PROGRESS – ANSWERS

1.2

a. Network is collection of machine which have been linked both physically and through software components to facilitate communication from sharing of information.

b. Protocol is set of rules for different computer machines, which determines how to communicate with each other through transmission media.

c. In client-server model data is kept on server. User can send request to server for sharing that data and called as client.

d. Server is a machine, which always process client's request, and sends response accordingly.

1) 1. Services
2. Client

2) 1 – b 2 – c 3 – a

1.3

a. Local area Network, Metropolitan Area Network, Wide Area Network, Wireless networks, Internet works.

b. The local area network is confined to a specific location such as a floor or any small area. It often used a transmission technology consisting of a single cable to which all machines are attached with each other. LANs runs at speed of 10 to 100 mbps have low delay and large very few errors.

c. A wide area network spans a large geographical area, often a country, or continent. It multiplies multiple Connected LANs that can be separated by any geographical distance. In most WANs the network contains numerous cables or telephone lines, each one connecting a pair of routers.

2) 1. 10 to 100 Mbps
2. MAN
3. routers and hosts

3) 1 – b 2 – c 3 – a

1.6 QUESTIONS FOR SELF – STUDY

Writes Notes on (Draw diagrams when necessary)

1. Types of networks
2. Client Server Model
3. Internetworks

1.7 SUGGESTED READINGS

1. Computer Networks : Andrew Tanenbaum
2. Networking Essentials : Emmett Dulaney

❁❁❁

NOTES

NOTES

Chapter 2

Basic Computer Networking

2.0 OBJECTIVES

After studying this chapter you will be able to-

- explain different types of computing.
- differentiate between centralize distributed and collaborative computing.

2.1 INTRODUCTION

Early chapter, we have seen that the types of network i.e. LAN, or WAN are establish for sharing data, to provide services, to allow for administration and security and to reduce equipment cost.

To achieve this centralized, Distributed and collaborative systems are use for computing of data.

Actual Network implementation can be done by using peer-to-peer, or server based networks.

Your Network can provide services like File, Print, Application and database etc.

Transmission media is a path way network entities use to contact each other. Computer transmission media includes cables and wireless technologies that allow network devices to contact each other. To reduce their design complexity most networks are organized as a series of layers or levels.

The Rules and conventions used in this convention are collectively known as layer protocol. Basically a protocol is an agreement between the communicating parties on how communication is to proceed.

A set of layers and protocol is called as Network architecture. A list of protocol used by a certain system, one protocol per layer is called as protocol.

2.2 ORGANIZATIONAL COMPUTATIONAL MODELS

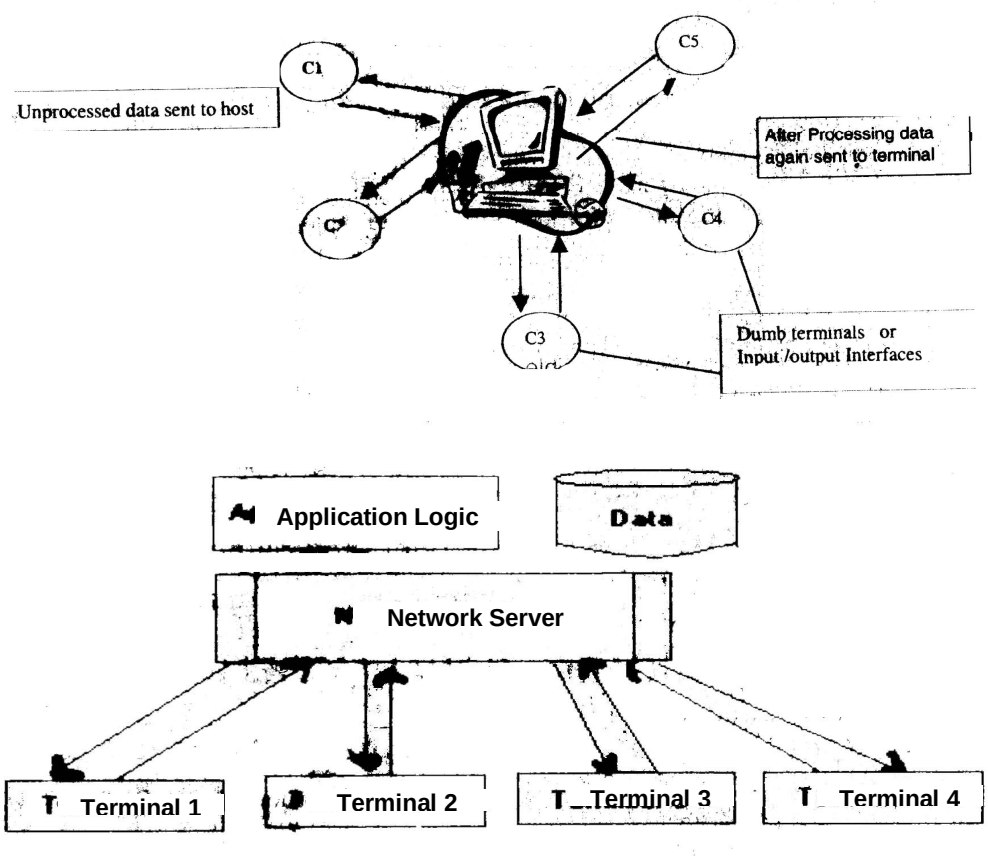
Whether a LAN or WAN, the overall goals of network are to establish a means of sharing data, to provide services, to allow for administration and security, and to reduce equipment cost. Three models, or methods of organization, are available for networking.

1. Centralized All processing is done at one location
2. Distributed Independent operation and local task
3. Collaborative Computers cooperate and share the load

2.2.1 Centralized computing

Centralized computing was the first method of networking implemented. As the name implies, all networking is done at one central location. The best example of this would be a UNIX host with a number of dumb terminals. The dumb terminals are nothing more than input/output interface into the host, and all processing actually takes place at the host. Because all interaction is at one location, all the terminals directly connected to the host and never connect with each other.

Whole processing of data will take place on centralize machine, but because of this system client's machine has to sent all data to central node, which will increase unnecessary traffic between server and client machine. As central machine has to respond each and every node speed of this system is low.



Centralize computing system

Merits of Centralize System

- Excellent security
- Centralize administration as both application logic and data resides on the same machine

Demerits of centralize system

* Mainframe computers are very expensive to buy, lease, maintain and use.
- The imitation is that both the application arid database live within the same machine process thereby offering no way to truly partition the application logic beyond the physical limitations of the mainframe.

2.2.2 Distributed Computing

With distributed computing, the dumb terminals are replaced PCs. The PCs can function separately and also interact with servers. Task are run locally, and data is exchanged, but without the server's performing any direction. A good, example of this scenario would be an NT server acting as file server with a number of Windows98 clients are capable of independent operations. The windows 98 clients are capable of independent operation. When they need to perform a task involving a file, they obtain it from server and perform the operation they need. The server gives them the file but doesn't tell them what to do with the data that was requested,

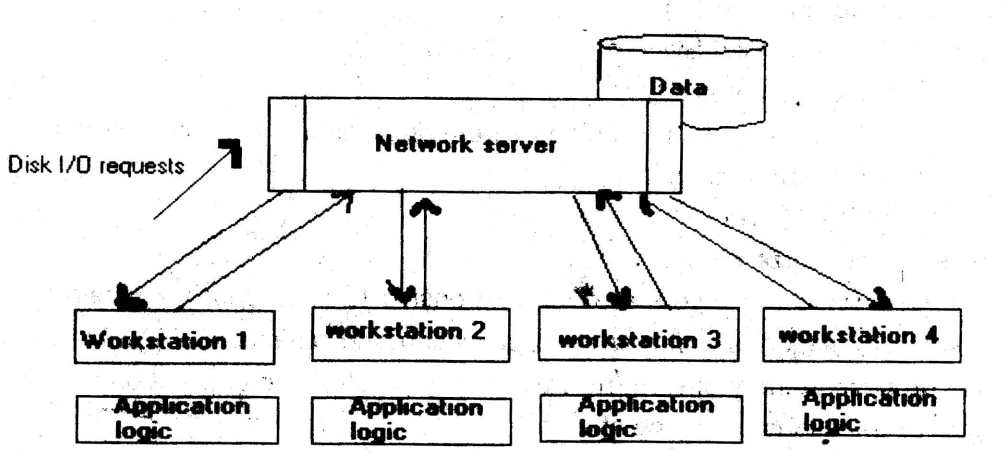
In this system application logic was executed of the client workstation instead of the server. These servers also provided access to computing resources like printers and large hard drives

Merits of distributed computing-

- Low cost entry point with flexible arrangement
- Computer resources can be added or reduced as and when necessary using this system.

Demerits of distributed computing

- As central administration is not there this will provide share level security.
- As client machine can do processing, client's machine need large amount of power to run the application.



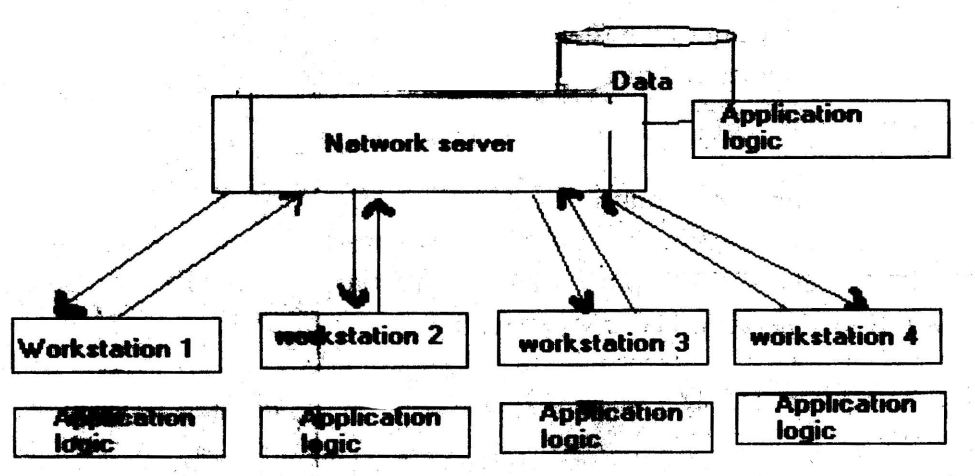
Taking into account the demerits of centralize system and distributed system architecture, collaborative computing architecture made its advent.

2.2.3 Collaborative Computing

Collaborative computers is also known as cooperative computing, enables computers to not only share resources (such as files) but also share processing. There are two methods by which this can invoke. A server might borrow an entire processor from an idle machine to perform an action, or the server might share part of processing with client.

A classic example of this environment is Microsoft SQL server. When a client requests data, SQL server does some of the processing an sends data to the client for

the completion of processing on that system. In all cases, the software must be written to take the advantage of absence of such software.



2.3 DIFFERENCE BETWEEN CENTRALIZE DISTRIBUTED AND COLLABORATIVE SYSTEM

Case study

Let us assume that we have a set of data stored in a database file namely student _info.mdb (Microsoft access file). This file holds the details of the marks stored in different -subjects by the students in their public examination. A client may want to know as to how many students have scored 100 percent in more than two subjects. A query is sent-to obtain the results. We shall discuss about the processing of the distributed and collaborative systems when a query to obtain the results satisfying the above-mentioned, criteria is issued.

1. Query sent to centralize system

In centralize type of computing server is a main, component all others are dump terminate or just input output nodes. Student_info database resides on centralize machine. Client's machine not hava any processing power. so query is sent to the server and server will do all the processing and processed results are sent to the client' machine.

2. Query sent to distributed system

In this case, the logic of query, is processed and evaluated at the client machine itself. The query logic realize that it needs to access a table namely student info in the MDB in order to process the request. Hence it requests the student_info table with all rows across the network before it applies the conditional clauses, which specifies the criteria that client is looking for.

So when SQL statement is used against a MOB, it is processed by the client machine and only a file I/O request is sent across the network to retrieve the required data in the from of disk blocks. No logic is executed at the server end except the transferring of file disk blocks. This is just a distributed computing.

3. Query sent to collaborative system

In collaborative architecture the actual SQL statement is sent across the network and processed by an application running locally on the server machine. As the SQL statement is processed on the server, only results need to send back to the client. This is a vast improvement over the distributed system. The query looking for student's detail having scored 100 % in two or more subjects is evaluated at the server end and only those records satisfying these criteria would be passed over the network instead of all records of the table.

Thus after receiving records from server, client's machine can perform rest of his work and display records satisfying condition to the user.

Check your Progress - 2.2

1) Answer in brief.

a. Explain the centralize computing?

……..……..……..……..……

……..……..……..……..……

2) Fill in the blanks

1. The collaborative computing is also known as …….. computing.
2. In centralized computing network is done at ……

2.4 NETWORKING MODELS

For actual network implementation we can use following networking models -

1. Peer-to-Peer Cheap to implement, minimal security
2. Server-based Requires a dedicated server and good security

2.4.1 Peer-to-Peer

In a Peer-to-Peer network you take the machine currently in existence, install networking cards in them, and connect them through some type of cabling. Each machine is known as Peer and can participate in the sharing of files or resources. No server is required, so there is no additional cost for a dedicated machine, but there is also no real security.

Peer-to-Peer networks require an operating system that can understand networking and function in this (Peer-to-Peer) way. Microsoft Windows 95, Microsoft Windows 98, Windows NT server and Windows NT workstation can all function in Peer to-Peer environment.

If file and print sharing has been enabled on a Windows 95 system, for example, you can create a share by selecting a folder and choosing to share it. By default, no password is associated with it but you can choose to assign one that a user must know in order to access the resource. Access permission can be Read-Only, Full or depend on password this is known as share level security. Access is gained when a user supplies the correct password to access the share.-

Peer-to-Peer networking works in small environments. If you grow beyond approximately 10 machines, the administrative overhead of establishing shares, coupled with the lack of tight security, creates a nightmare.

Advantages of peer-to-peer network

- Server is not required
- No additional cost for dedicated-machine

Disadvantages of peer-to peer network

- Provides share level security
- Can work in small environments only.

2.4.2 Server Based

In the presence of server, be it on NetWare Or NT, you can implement user

level security on your network. With the user level security, permissions are based *on* how the user logged on and was authenticated by the server. Every user has an account. In this environment, you can assign permissions to shared based on user permissions or group permissions. In short you must have server on the network in order to have user level security, but you can have share level security with or without server.

This scenario also known as client/server networks (explain previously in chapter 1), server-based networking's down side is that it requires a dedicated machine (the server); the upside is that you gain centralize administration, you can add ail users at one location, control logon scripts and backups; and so on. With centralized authentication, you can identify a user to your entire network based on his logon name and password, not based on each share he attempts to access.

Advantages of Server based network

• Provides user level security

• You always gain centralize administration

• Can work in big environments also

Disadvantages of server based network

- Dedicated machine is required
- Cost of the system is more compared to peer-to peer networks.

-. Peer-to-Peer networks can exists comfortably within server-based networks. In many business combinations of two models are used. A server-based network is used to provide e-mail; and other resources to all users, and Peer-to-Peer networks are established within divisions to share resource among select users.

Microsoft, also calls Pee-to-Peer networks workgroup and server- based networks domains. These terms are used interchangeably in almost air Microsoft documentation.

Check your Progress-2.3

1) Explain in brief.

1. Domain

   ……..……...…….

   ……..……...…….

2. Workgroup

   ……..……...…….

   ……..……...…….

2) Fill in the blanks.

1. Server based network provides …… security
2. Protocol is an agreement between ……..

2.5 NETWORK SERVICES

In the previous topic we, discussed about server and client model as well, as advantages, of server, a server is a machine that provides resources, and every machine accessing those resources is known as client. There are different types of servers. The three most common are file, print and application servers.

A. File Servers

File servers store files on the network for clients to access. In so doing they provide a central location where a number of users can find the same data. All users can see the same information at same time with help of file server, they also provide a central point for backup operations and simplify the work. In this way as every file is on serve and server provides user level security the data is kept safe.

B. Print server

Print servers, as name implies, offer printing services to clients. A single print server offers access to one or more printers to uses the term file and print server generically to mean any server that offers file services, print services or both.

C. Application Server

An application server can run all or some of an application for a client. Not only does it hold data in the file server, but also it has the application needed to process the data. After all or some of the processing is complete at the server, the results are downloaded to the client.

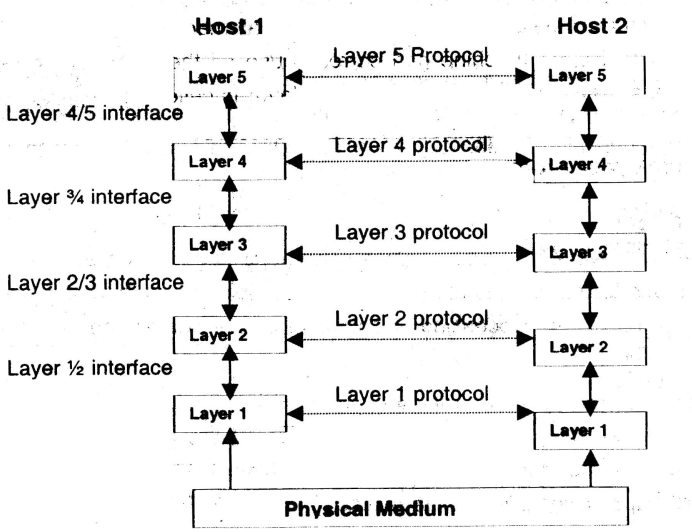
To compare the three, the file and print servers offers a storage location for the clients. They therefore benefit greatly from large hard drives. Although RAM is important the processor is not so important, an application server on other hand requires fast processor to run the application and get the results to the client. RAM is also important to the application server, while the size of the hard drive is usually not (within reason)

2.6 TRANSMISSION MEDIA AND PROTOCOL

Transmission media is a pathway network entities use to contact each other. Computer transmission media includes cables & wireless technologies that allow network devices to contact each other .To reduce their design complexity most networks are organized as a series of layers or levels. Each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer and the function of each layer differ from network to network. However, in all networks, the purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services actually implemented.

Layer n on one machine carries on a conversation with layer n on another Machine. The rules and conventions used in this conversation are collectively known as n protocol. Basically a protocol is an agreement between the communicating parties on how communication is to proceed. Violating the protocol communication more difficult, if not impossible.

A five-layer network is illustrated as below. The entities comprising the corresponding layers on different machines are called peer. In other workds, it is the peer that communicate using the protocol.



In reality no data are directly transferred from layer n on one machine to layer n on another machine. Instead each layer passes data and control information to the layer immediately below it, until the lowest layer is reached. Below layer 1 is the physical medium through which actual communication occurs. In the diagram virtual communication is shown by dotted lines and physical communication by solid lines.

Between each pair of adjacent layers there is an interface. The interface defines which primitive operations and services the lower layer offers to the upper one. When network, designers decide how many layers to include in a network and what each one should do, one of the most important consideration is defining clean interfaces between the layers. Doing, so in turn, requires that each layer perform a, specific collection of well-understood functions. In addition to minimizing the amount of information that must be passed between the layers, clean-cut interfaces also makes it simpler to replace the implementation of one layer with a completely different implementation (for Eg, all the telephone lines are replaced by satellite channels) because all that is required of the new implementation is that it offers exactly the same amount of services to its upstairs neighbor as the old implementation did.

A set of- layers and protocol is called as network architecture. The specification of an architecture must contain enough information to allow an implements to write the program or build the hardware for each layer so that it will correctly obey the appropriate protocol. It is not event necessary that the interfaces on all machines in a network be the same, provided that each machine can correctly use all the protocols. A list of protocols used by a certain system, one protocol per layer is called as protocol stack.

Check your Progress -2.4-2.5-2.6

Answer in brief.

1. What is transmission media?

   ……..……..……

   ……..……..……

2. What is protocol?

   ……..……..……

   ……..……..……

3. Define network architecture?

   ……..……..……

   ……..……..……

4. Explain the use of file service?

   ……..……..……

   ……..……..……

2.7 SUMMARY

In this we have studied centralized, Distributed and collaborative systems are use for computing of data. Actual Network implementation can be done by using peer-to-peer, or server based networks. Your Network can provide services like File, Print, Application and database etc.

Transmission media is a pathway network entities use to contact each other. Computer transmission media includes cables & wireless technologies that allow network devices to contact each other .To reduce their design complexity most networks are organized as a series of layers or levels.

The rules and conventions used in this conversation are collectively known as layer n protocol. Basically a protocol is an agreement between the communicating parties on how communication is to proceed. Violating the protocol will make

communication more difficult, if not impossible.

A set of layers and protocol is called as network architecture. A list of potocols used by a certain system, one protocol per layer is called as, protocol.

Source : *nptel.iitm.ac.in(E-book)*

2.8 CHECK YOUR PROGRESS – ANSWERS

1. **Centralize computing-:** all networking done at one central location. In this all input / output interfaces are connected to central machine. The method provides excellent security and central administration as both data and application logic resides on central machine. On other hand centralize machine is very costly to buy. As central machine has to respond every node speed of this system is low.

2) 1. Cooperative 2. One central location

2.3

1)

1. Domain- domain is nothing but the server on the network in order to have user level security. With the user level security, permissions are based on how the User logged ort and was authenticated by the server.

2. Workgroup-: In peer-to-peer networks, by installing network card in machines and connect them through some type of cabling, can participate in the sharing of files or resources. Such system of networking is called as workgroup. Merits of Server-based network-

- Provides user level security.
- You always gain centralize administration,
- Can work in big environments also. Demerits of peer-to-peer network-
- Provides share level security
- Can work in small environments only.

2) 1) User Level 2) Communicating Parties

2.4 , 2.5 &2.6

1. Transmission media is a pathway to network -entities use to contact each other.
2. A set of rules for different computer machine which determines how to communicate with each other through transmission media, is called as protocol.
3. Network architecture-: A set of layers and protocol is called as network architecture.
4. File server stores files on the network for clients to access. They provide a central location *to* find data. All users can see same information at same time. They, also provide central point for back operations.

2.9 QUESTIONS FOR SELF – STUDY

I. Answer the following questions.

1. Why server based networks are preferred?
2. What is protocol stack?
3. Define layer?

4. Explain demerits of centralized computing?
5. List different network services?

II. Write notes on the following.

1. Relation between Transmission media and protocol
2. Network services
3. Distributed computing
4. Peer to peer networks
5.

2.10 SUGGESTED READINGS

1. Computer Networks : Andrew Tanenbaum
2. Remote Access Study Guide : Robert Padjen, Todd Lammle, Sean Odom

❁❁❁

Chapter 3

Transmission Media

3.0 OBJECTIVES

After studying this chapter you will be able to -

- ✓ explain transmission media
- ✓ discuss how choose proper transmission media according to characteristics
- ✓ explain what type of cable media we can use for transmission of data
- ✓ describe wireless media

3.1 INTRODUCTION

Present day computer use electronic currents, radio waves, microwaves or light spectrum energy from electromagnetic spectrum to transmit signals.

Computers use electronic voltage pulses or electromagnetic waves (EM) to send signals for the following reasons

- They are available in form of electric currents.
- They can be altered by semiconductor materials
- They can be used to represent at least two discrete states (binary / Digital). The physical path through which the electrical voltages and EM waves travel is called Transmission Media. In other words transmission media make possible the transmission of the electronic signals from one computer to another computer. It is through the transmission media that networked computers signal each other. Computer networks rely upon the ability of transmission medium to

accommodate, a range of electric voltages or EM waves. Different media are used to transmit the signals, depending on the frequency of EM waveform .

The following table gives the frequency range for each portion of EM spectrum.

No	Signal Type	Frequency range	Applications
1.	Electric current / Voltage	1Hz-10KHz	Power and telephone
2.	Radio waves	10 KHz – 300 MHz	Radio And TV
3.	Microwaves	1GHz – 300 GHz	Satellite Communication
4.	Infrared	1THz - 30THz	Remote control for TV etc.

Transmission media can be classified as cable (bounded) or wireless (unbounded). Cable media provide a conductor for the electromagnetic signal while wireless media do not. The examples of bounded media are twisted pair cable, coaxial cable and fiber cable; while that unbounded media are radio waves microwaves and infrared. Bounded media are radio waves microwaves and infrared. Bounded media are normally used in both LAN and WAN, white unbounded media are essential for networks with mobile computer and mobile phones and also are widespread to enterprise the global networks.

3.2 CHARACTERISTICS OF TRANSMISSION MEDIA

Each type of transmission media has special characteristics that make it suitable for specific type of service. Each media type should be discussed keeping the following factors in the mind:

- Cost
- Capacity (bandwidth)
- Ease of installation
- Attenuation
- Immunity from electromagnetic interference (EMI)

3.2.1 Bandwidth

In computer networking, the term bandwidth is refers to as the measure of the capacity of a medium to transmit 'data. A medium that has a high capacity, has high bandwidth, whereas a medium that has limited capacity has low bandwidth. Bandwidth can be best- understood by comparing it to its hose. If half-inch garden hose can carry water from a trickle up two gallons per minute, that hose can be said to have a bandwidth gallon's per minute. A four-inch fire hose, however, might have a bandwidth that exceeds 100 gallons per minute.

Data transmission rates are frequently stated in terms of bits that can be transmitted per second. An Ethernet LAN theoretically can transmit 10 - million bits per second and has a bandwidth of 10 megabits per second (Mbps).

The bandwidth that a cable can accommodate is determined in part by the cable's length. A short cable generally can accommodate greater bandwidth than a longer cable, which is one reason why all cable designs specify maximum length for cable runs. Beyond those limits, the highest-frequency signals can deteriorate, and errors begin to occur in data signals.

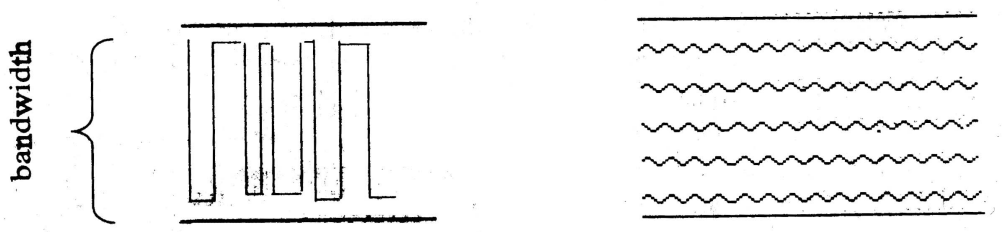
The two ways to allocate the capacity of transmission media are with baseband and broadband transmissions. Baseband devotes the entire capacity of the medium to one communication channel. Broadband lets two or more communication channels share the bandwidth of the communication medium. Baseband is the most common mode of operation. Most LANs function in baseband mode, for Sample baseband signaling can be accomplished with both analog digital signals.

Although you might not realize it, you have a great deal of experience with broadband transmission. Consider for example, that the TV cable coming into your house from an antenna or cable provider is a broadband medium. Many television signals, can share the bandwidth of cable because each signal is modulated using a separately assigned frequency. You can use the television tuner to choose the channel you want to watch by selecting its frequency; This technique of dividing bandwidth into frequency band is called as frequency division multiplexing (FDM) and works only with analog signals. Another technique, called time division multiplexing (TDM), also supports digital signals.

3.2.2 Multiplexing

Multiplexing is a technique that allows broadband media to support multiple data channels. Multiplexing makes sense only under a number of circumstances :

1. When media bandwidth is costly. A high-speed leased line, such as a T1 or T3, is expensive to lease. If the leased line has sufficient bandwidth, multiplexing can allow the same line to carry mainframe, LAN, voice, videoconferencing, and various other data types.
2. When bandwidth is idle. Many organizations have installed fiber optic cable that is used only to partial capacity. With the proper equipment, a single fiber can support hundreds of megabits- or even a gigabit or more of data.
3. When large amounts of data must be transmitted through low capacity channels. Multiplexing techniques can divided the original data stream into several lower-bandwidth channels, each of which can be transmitted through a lower capacity medium. The signals can then be recombined at the receiving end.



Baseband **Broadband**

Multiplexing refers to combining multiple data channels for transmission on common medium. from medium. Demultiplexing refers to recovering the original separate channels from multiplexed signal. Multiplexing and demultiplexing performed by a multiplexor, which usually have both capabilities.

Frequency division multiplexing (FDM)

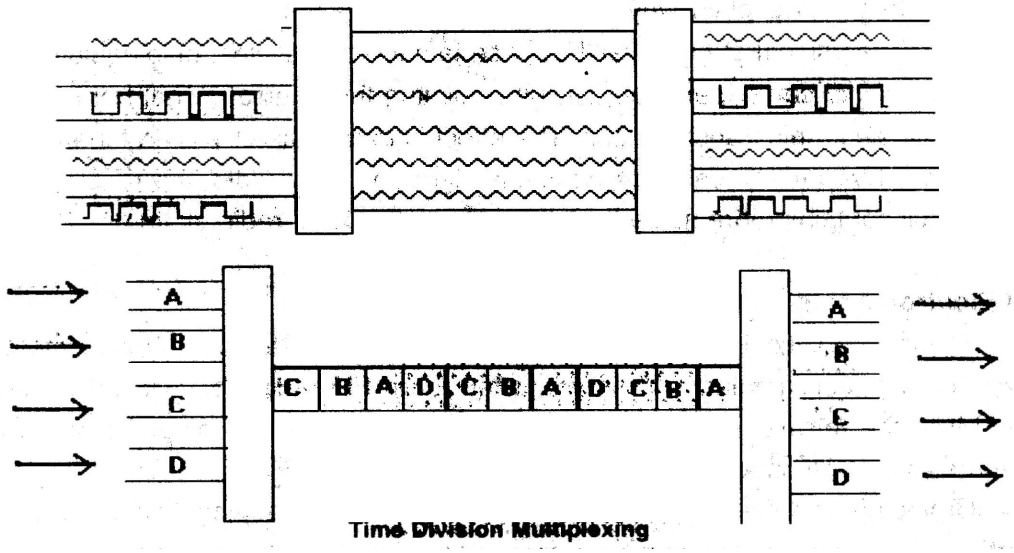
This technique works by converting all data channels to analog form. Each analog signal can be modulate by a separate frequency (called a carrier frequency) that makes it possible to recover that signal during the demultiplexing process. At the receiving end the demultiplexor can select the desired carrier signal and use it to extract the data signal and use it to extract the data signal from the channel.

FDM can be used in broadband LANs (a standard for Ethernet also exist) one advantage of FDM is that it supports bi-directional signaling on the same cable.

Time Division Multiplexing- (TDM)

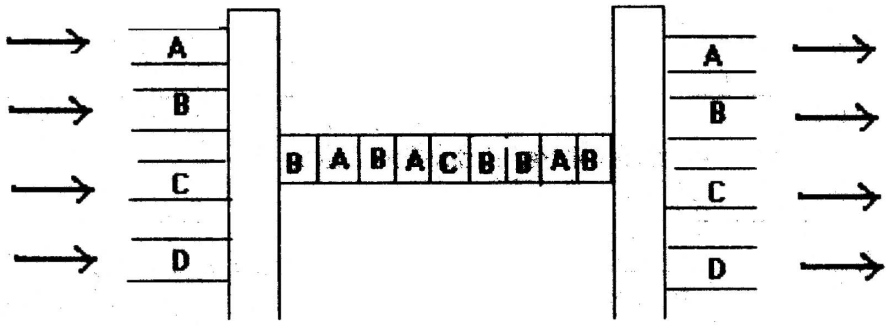
Time Division Multiplexing divides a channel into time slots that are allocated to the data streams to be transmitted, as shown in diagram below. If the sender and receiver agree on the time-slot assignments, the receiver can easily recover and reconstruct the original data streams.

Time Division Multiplexing transmits the multiplexed signals in baseband mode. Interestingly, this process makes it possible to multiplex a TDM multiplexed signal one of the data channels on an FDM system. Conventional TOM equipment utilizes fixed time-divisions and allocated time to a channel, regardless of that channel's level of activity. If the channel is not busy, its time slot not being fully utilized.



Time Division Multiplexing

Because the time divisions are programmed into the configurations of the multiplexors, this technique; often is referred to as Synchronous Time Division Multiplexing. If using the capacity of data medium more efficiently is important, amore sophisticated technique, Statistical Time Division Multiplexing, can be used. A stat-mux uses the time slot technique but allocates time slots based on the traffic demand$_r$pn the individual channels. As shown in figure. Notice that Channel B is allocated more time slots than Channel A and channel C is allocated the fewest time slots. Channel D is idle, so no slots are allocated to it. To make this procedure to work, the data transmitted for each time slot includes a control field that identifies the channel to which the data in the time slot should be assigned.



Statistical time-division multiplexing

3.2.3 Attenuation

Attenuation is a measure of how much a signal weakens as it travels through a medium. This chapter doesn't discuss attenuation in formal terms, but it does address the impact of attenuation on performance. Or Attenuation is a contributing factor to explain why cable designs must specify limits in the lengths of cable runs. When signal strength fall below certain limits, the electronic equipment that receives the signal can

experience difficulty isolating the original signal from the noise present in all electronic transmissions. The effect is exactly like trying to tune in distant radio signals. Even if you can lock on to the signal on your radio, the required sound generally still contains more noise than the sound from local radio station.

3.2.4 Electromagnetic Interference (EMI)

Electromagnetic interference consists of outside electromagnetic noise that distorts the signal in medium. When you listen to an FM radio, for example you often hear EMI in the form of noise caused by nearby motors or lightning. Some network media are more susceptible to EMI than others.

Cross talk is a special kind of interference caused by adjacent wires. Cross talk is particularly significant problem with computer networks, because large numbers of cables are often located close together with minimal attenuation to exact placement. The purpose bf transmission media is to transport a raw data from one machine to another. Various physical media can be use for this type of transmissions. Each one has its own niche in in terms of bandwidth, delay, cost and ease of installation and maintenance. Media are roughly grouped into cable media and wireless media. Considering all above factors you -have to select proper transmission media, which will satisfy the needs of networking.

3.1 – 3.2 Check your progress.

Answer in brief.

1. Define transmission media?

   ……

   ……

2. What are the characteristics of transmission media?

   ……

   ……

3. What is time division multiplexing?

   ……

   ……

4. Explain the phenomenon of Attenuation?

   ……

   ……

5. What is purpose of transmission media?

   ……

   ……

6. What is electromagnetic interference?

   ……

   ……

3.3 CABLE MEDIA

* Coaxial Cable
* Fiber optic cable
* Twisted-pair

3.3.1 Coaxial Cables

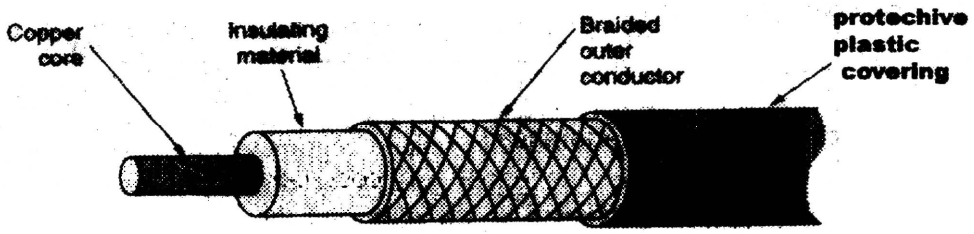
Coaxial cables were the first cable types used in LANs. Coaxial cable gets its name because two conductors share a common axis. The cable is most frequently referred as coax. It has better shielding than twisted pair, so it can span longer distances at higher speed two kinds of co-axial cable are widely used.

1. 50-ohm cable (Base band coaxial cables / Thinnet) is commonly used for digital transmission.
2. 75-ohm cable (Broad band coaxial cables / thicknet) is commonly used for analog transmission.

This distinction is based on historical, rather than technical, factors (e.g.- early dipole antennas had an impedance of 300 ohms, as it was easy to built 4:1 impedance matching transformers)

The components of the co-axial cable are as follows:

- A central conductor, although usually solid copper wire, this sometimes is also made of standard wire.
- An outer conductor forms a tube surrounding the central conductor. This conductor can consist of braided wires, metallic foil or both. The outer conductor, frequency called the shield, servers as a ground and also protects the inner conductor from EMI.
- An insulation layer keeps the outer conductor spaced evenly from the inner conductor.
- A plastic encasement (jacket) protects the cable from damage.



coaxial cable.

The construction and shielding of the co-axial cable give it a good combination of high bandwidth and excellent noise immunity. The possible bandwidth depends on the cable length.

Types of Co-axial cables

Baseband Co-axial cables (Thinnet)

This is light and flexible cabling-medium that is inexpensive and easy to install. Following table illustrate some thinnet classifications. Note that thinnet falls under the RG-58 family, which has 50 ohm impedance. Thinnet is approximately .25 inches (6 mm) in thickness.

Cable	Description	Impedance
RG-59/U	Solid copper centre	50 ohm
RG-58A/U	Wire stand centre	50 ohm
RG-58C/U	Military version of RG-58 A/ U	50 ohm

Thinnet cable can reliably transmit a signal for 185 meters (about 610 feet). Although it's called 10Base2 to give the impression that it can run 200 meters, this is

erroneous. It should really be called 10Base 1.85.

Broadband Co-axial cables (Thicknet)

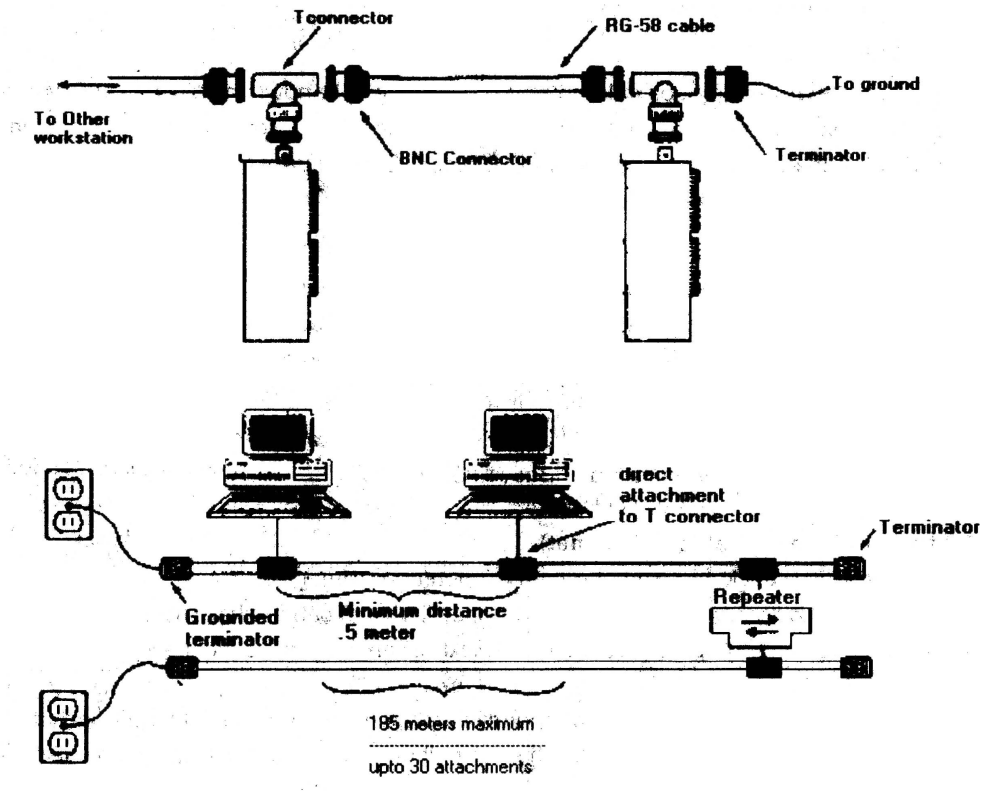
Thicknet is thicker in diameter that thinnet (approximate 0.5 inches). Because it is thicker and doesn't bend as readily as Thinnet. Thicknet cable is harder to work with. A thicker center core, however, means that Thicknet can carry more signals for a grater distance than Thinnet. Thicknet can transmit a signal approximately 500 meters (1650 feet). Thicknet cable is sometimes called Standard Ethernet (although other cabling types are also useful for Ethernet) Thicknet can be used to connect two or more small thinnet LANs into a larger network. Because of its greater size, Thicknet is also more expensive than thinnet It can be installed, safely outside, running from building to building, such as with cable TV.

Co-axial Characteristics

You should be familiar with the installation cost. Bandwidth and EMI cost, bandwidth and EMI resistance characteristics of coaxial cable.

A. Installation

Co-axial cable typically is installed in two configurations: daisy chain (from device to device-Ethernet) and star (ARC net)



The Ethernet cabling shown in the figure is an example of Thinnet, which uses RG-58 cable. Devices are connected to the cable by means of T. connectors. Cables are used to provide connections between T-Connectors. One characteristic of this type of cabling is that a special connector, called terminator, must terminate the ends of cable run. The terminator contains a resistor that is-matched to the characteristics of the cable. The resister prevents signals that reach the end of the cable from bouncing back and causing interference.

Co-axial cable is reasonably easy to install because it is robust and difficult to damage. In addition, connectors can be installed with inexpensive tools and a bit of practice. The device -to-device cabling approach can be difficult to reconfigure, however, when new devices cannot installed near an existing cabling path.

The co-axial cable used for Thinnet fall at the low end of the cost spectrum, whereas Thicknet is among the more costly options.

Bandwidth -

LANs that employ coaxial cable typically have a bandwidth between 8.5 mbps and 10 Mbps. Thicker co-axial cables offer higher bandwidth, and the potential bandwidth of co-axial is much higher than 10 Mbps. Current LAN technologies, however don't take advantage of take of this potential.

EMI characteristic

All copper media are sensitive to EMI, although the shield in coax makes the cable fairly resistant, Coaxial cables, however, do radiate a portion of their signal, and electronic eavesdropping equipment can detect this radiated signal.

Connectors for Coaxial cables

Two types of connectors are commonly used with coaxial cable. The most common is the BNC corrector mainly used for thinnet cabling. In contrast Thicknet uses N-Connectors, which Screw instead of using a twist lock.

3.3.1. Check your progress.

1. Explain, difference between broadband and baseband coaxial cables?

   ……

   ……

2. What are important parts of co-axial cable?

   ……

   ……

3. Which types of connectors are required for co-axial cable?

   ……

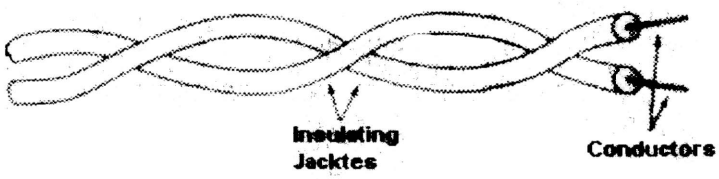
   ……

3.3.2 Twisted pair

Although the bandwidth characteristics of magnetic tapes are excellent, the delay characteristics are poor. Transmission time is measured in minutes or hours, not milliseconds. For many applications an online connection is needed. The oldest and still most common transmission medium is twisted pair, which employs copper cable. One more reason for popularity of twisted pair is low cost. This type of cable is inexpensive to install and offers the lowest cost per foot of-any cable type.

A basic twisted pair cable consists of two strands of copper wire twisted together, as shown below. This twisting reduces the sensitivity of the cable to EMI and also reduces the tendency of the cable to radiate radio frequency noise that interferes with nearby cables and electronic components. This is because the radiated signals from the twisted wires tens to cancel each other out. Antennas, which are purposely designed to radiate radio frequency signals, consist of parallel, not twisted wires)

Twisting also controls the tendency of the wires in the pair to cause EMI each other. Whenever two wires are in close proximity, the signals in each wire tend to produce noise, called crosstalk, in the other. Twisting the wires in the pair reduces crosstalk in much the same *way* that twisting reduces the tendency of the wires to radiate EMI.



Twisted pair Cable

Two types of twisted-pair cable are used in LANs :

- Shielded
- Unshielded

Shielded Twisted-Pair (STP) Cable

Shielded twisted-pair cabling consists of one or more twisted pairs of cables enclosed in a foil wrap and woven copper shielding as shown above. Diagram shows IBM type 1 cabling, the first cable type used with IBM token Ring. Early LAN designers used shielded twisted-pair cable because shield further reduces the tendency of the cable to radiate EMI and thus reduces the cable's sensitivity to outside interference.

Co-axial and STP cable used shields for the same purpose. The shield is connected to the ground is a portion of the electronic device to which the cable is connected. A ground is a portion of the device that serves as an electrical reference point. Usually it literally connected to a metal stake driven into the ground. A property grounded shield prevents signals from getting in to or of the cable.

In IBM Type 1 cable include twisted pairs of wire within a single shield Various types of STP cable exist. Some shield each pair individually, and others shield several pairs. The engineers who design a network's cabling system choose the exact configuration. IBM design, and each several twisted pair cable types to use with their Token ring network design, and each cable type is appropriate for a given kind of installation.

STP cables cost more than thin coaxial or unshielded twisted pair cable. STP is less costly, than thick coax or fiber-optic cable.

Capacity

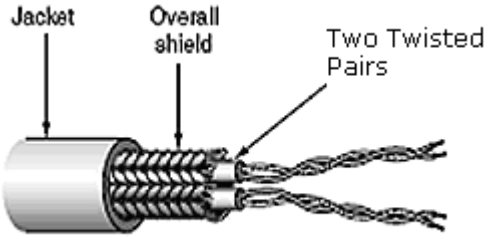
STP cable has a therotical capacity of 500 Mbps, although few implementations exceed 153 Mbps with 100 meters cable runs. The most common data rate for STP cable is 16 Mbps, which is the top data rate for token Ring networks.

Attenuation

All varieties of twisted-pair cable have attenuation characteristics that limit the length pf cable runs to a few hundred teeters, although a 100-flfteter limit is most common.

EMI characteristics

The shield in STP cable results in good EMI characteristic for copper cable, comparable to the EMI characteristic of coaxial cable. This is one reason STP might be preferred to unshielded twisted-pair cable in some situations. As with all copper cables. STP is sensitive to interference and vulnerable to electronic eavesdropping.



A Shielded Twisted-Pair Cable

Unshielded Twisted-pair (UTP) cable

Unshielded Twisted-pair cable does not incorporate a braided shield into its structure; however, the characteristics of UTP are similar in many ways to STP, differing primarily in attenuation and EMI. As shown in figure, several Twisted-pairs can be bundled in a single cable. These pairs typically are colour-coded to distinguish them.

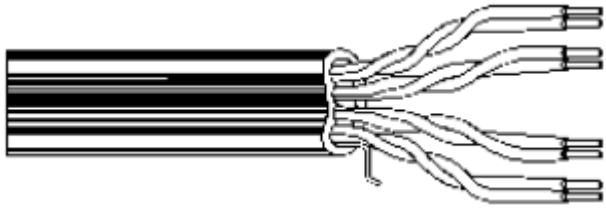
Telephone systems commonly use UTP cabling. Network engineers can sometime use existing UTP telephone cabling (if it is new enough and of high-enough quality to support network communications) for network cabling.

UTP cable is a latecomer to high-performance LANs because engineers only recently solved the problems of managing radiated noise and susceptibility to EMI. However, a clear trend toward UTP is in operation, and all new copper based cabling schemes are based on UTP.

UTP cable is available in the following five grades, or categories :

- **Categories 1 and 2 -** These voice-grade cables are suitable only for voice and for low rates (below 4 mbps). Category 1 was once the standard voice-grade cable for telephone systems. The growing need for data-ready cabling systems, however, has caused Categories 1 and 2 cables to be supplanted by category 3 for new installation.
- **Category 3 -** As the tower data-grade cable, this type of cable generally is suited for data rates 10 mbps. Some innovative schemes, however, let the cable support data rates up to 100 mbps. Category 3, which uses four twisted pairs with three twists per foot, is now the standard cable used for most telephone installations.
- **Category 4 -** This data grade cable, which consist of four twisted pairs, is suitable for data rates up to 16 Mbps.
- **Category 5 -** this data grade cable, which also consist of four twisted pairs, is suitable for data range up to 100 mbps. Most new cabling systems; for 100 Mbps data rates designed around Category 5 cable.

DTP cable offers an excellent balance of cost and performance characteristics, a discussed in the following sections.



Multi Pair UTP cable

Cost

UTP cable is the least costly of any cable type, although properly installed Category 5 tends to be fairly expensive. In some cases existing cable in buildings can be used for LANs, although you should verify the category of the cable and know the length of the cable in the walls. Distance limits for voice cabling are much less

stringent than for data-grade cabling.

Installation

UTP cable is easy to install. Some specialized equipment might be required, but the equipment is low in cost and can be mastered with a bit of practice. Properly designed UTP cabling systems easily can be reconfigured to meet changing requirements.

As noted earlier, however, Category 5 cable has stricter installation requirements than lower categories of UTP. Special training is recommended for dealing with Category 5 UTP.

Capacity

The data- rates possible with UTP have increase from 1 Mbps; pat 4 and 16 Mbps, to the point where 100 Mbps data rate are now common,

Attenuation

UTP cable share similar attenuation characteristics with other copper cables. UTP cable runs are limited to a few hundred meters, with 100 meters as the most frequent limit.

EMI Characteristics

Because DTP cable lacks a, shield, it is more sensitive to EMI than coaxial or STP cables. The latest technology makes it possible to use UTP in the vast majority of situation, provided that reasonable care is taken to avoid electrically noisy devices such as motors and fluorescent lights. Nevertheless, UTP might not be suitable for noisy environments such as factories. Cross talk between nearby unshielded pairs limits the maximum length of cable runs.

Connectors for UTP

The most common connector use with UTP cables is the RJ-45 connector. These connectors are easy to install on cables and are also extremely easy to connect and disconnect.

Advantages of UTP cable

- Relatively inexpensive
- Easily installed, managed, and reconfigured
- Basic technology and standards are matured and stable

Disadvantages of UTP cable

- Only categories 5,6,7 UTP cables are capable of high-speed (> 100 Mbps) data transmission.
- Relatively high rate of attenuation
- Sensitive to EMI

Check your progress.

1. Explain the capacity of UTP and STP cables?

   ……

   ……

2. Note down the advantages and disadvantages of UTP cables?

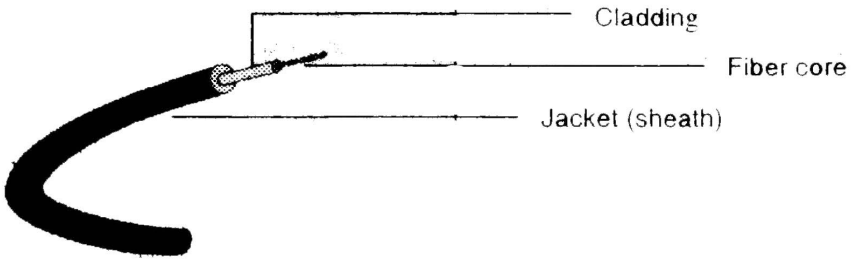
   ……

   ……

3.3.3 Fiber-Optic cable

In almost every way, fiber-optic cable is the ideal cable for data transmission. Not only does this type of cable accommodate extremely high bandwidth's, but it also presents no problems with EMI and supports durable cables an cable runs as long as several kilometers. The two disadvantages of fiber-optic, however, are cost difficulty of installation.

The center conductor of a fiber-optic cable is a fiber that consists of highly refined glass or plastic designed to transmit light signals with little loss. A glass core supports a longer cabling distance, but a plastic core is typically easier to work with. The fiber is coated with a cladding that reflected signals back into the fiber to reduce signal loss. A plastic sheath protects the fiber. See Figure



Optical fibers are much smaller and more lightweight than copper wires. Therefore, large fiber optic cables carry more conductors than similar sized copper cables. There are two types of optical fibers. 1. Multimode fiber 2. Single mode fiber

The following table shows the comparison between single mode and multimode fibers

Sr. No	Single mode Fiber	Multimode Fiber
1	High capacity	Lesser capacity than single mode
2	More costlier	Cheaper than single mode
3	Light pulses are generated by injection Laser diode (ILDs)	Light pulses are generated by light emitted diodes (LEDs)
4	Can sustain a transmission rate of 100 Mbps at distance of 20 KM	Pan sustain a transmission rate of 100 Mbps at distance of 2 KM
5	Has been, optimized to allow one light path	Has been optimized to multiple one light path

A fiber-optic network cable consists of two strands separately enclosed in plastics sheaths- one strand sends and the other receives. Two types of cable configuration are available:

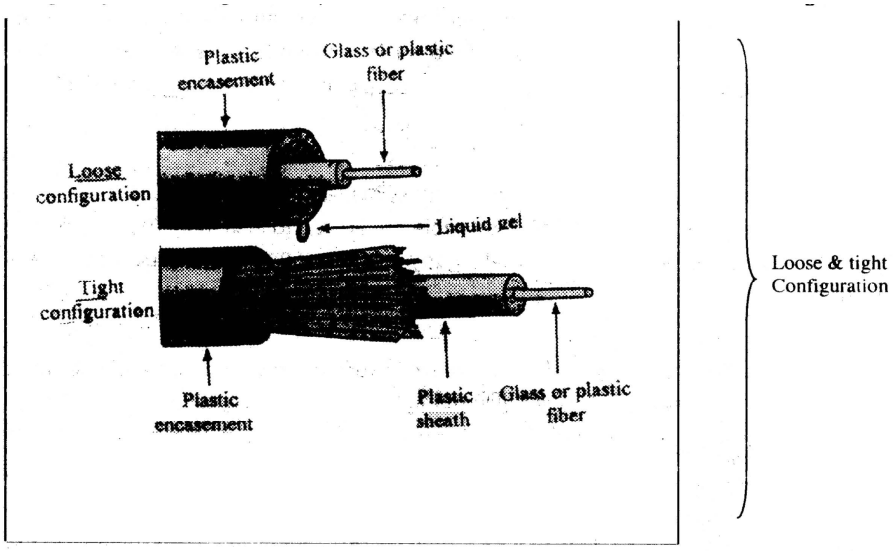
- **Loose configuration**

Loose configuration incorporates a space between the fiber sheath and the outer plastic encasement; this space is filled with gel or other material.

- **Tight configuration**

Tight configuration contains strength wires between the conductor and the outer plastic encasement.

In both cases, plastic encasement must supply the strength of the cable, while the get layer or strength wires protect the delicate fiber from mechanical damage.



Fiber optic cable doesn't transmit electrical signals. Instead, the data signals must be converted into light signals. Light sources include lasers and light-emitting diodes (LEDs). LEDs are inexpensive but produce a fairly poor quality of light suitable for less-stringent application. The end of the cable that receives the light signal must convert the signal back to an electrical form. Several types of solid-state components can perform this service.

One of the significant difficulties of installing fiber-optic cable arises when two cables must be joined. The small cores of the two cables (some are as small as 8.3 microns) must be lined up with extreme precision to prevent excessive signal loss.

As with all cable types, fiber-optic cable has their share of advantages and disadvantages.

Cost

The cost of the cable and connector has fallen significantly in recent years. However, the electronic devices required are significantly more expensive than comparable devices for copper cable. Fiber-optic cable is also the most expensive cable type to install.

Installation

Greater skill is required to install fiber-optic cable than to install most copper cables. However, improved tools and techniques have reduced the training required. Still, fiber-optic cable requires greater care, because the cable must be treated fairly gently during installation. Every cable has a minimum bend radius, for example, and fibers are damaged if the cables are bent too sharply. It is also important not to stretch the cable during installation.

Capacity

Fiber-optic cable can support high data fates (as high as 200,000 Mbps), even with long cable runs. Although UTP runs cable are limited to less than 100 meters with TOO Mbps data rates, fiber optic cable can transmit 100 Mbps signals for several kilometers.

Attenuation

Attenuation in fiber-optic cables is much lower than in copper cables. Fiber-optic cables can carry signals for several kilometers.

EMI Characteristics

Because fiber-optic cable doesn't use electrical signals to transmit data, they are totally immune to electromagnetic interference. These cables are also immune to a variety of electrical effects that must be taken into account when designing copper cabling systems.

Because the signals in fiber-optic cable are not electrical in nature, they cant be detected by the electronic eavesdropping equipment that detects electromagnetic radiation. Therefore, fiber-optic cable is the perfect choice for high-security networks.

Advantages of Fiber optic cable

- Supports very high bandwidth- from 100 Mbps to >2Gbps
- Very low alteration
- Immune to EMI or eavesdropping

Disadvantages

- Very expensive cables
- More complex to install
- High precision required for connections

Cheek your progress.

1. Differentiate between loose configuration and tight configuration?

   ……

   ……

2. Explain the advantages and disadvantages of fiber optic cable?

   ……

   ……

3.4 WIRELESS MEDIA

Our age has given rise to in formation junkies: people who need to be online all the time. For these mobile users, twisted pair, coax, and fiber optics are of no use. They need to get their hits of data for their laptop, notebook or palm top. Without being depending on the terrestrial communication infrastructure, for these users wireless communication is the answer. In this section we will look at wireless communication in general, as it has many other important applications besides providing connectivity to users who want to read their e-mail in airplanes. Technology is expanding rapidly and will continue to expand into the near future, offering *more* and better options for wireless networks.

Presently, you can subdivide wireless networking technology into three basic types that corresponds to three basic networking scenarios :

- **Local area networks (LANs)**

Occasionally you will see a fully wireless LAN, but more typically, one or more wireless machines will function as members of cable-based LAN. A LAN with both wireless and cable-based components is called as hybrid.

- **Extended local networks**

  A wireless connection serves as a backbone between two LANs, For instance, a company with office networks in two nearby but separate buildings could connect those networks using a wireless bridge.

- **Mobile computing**

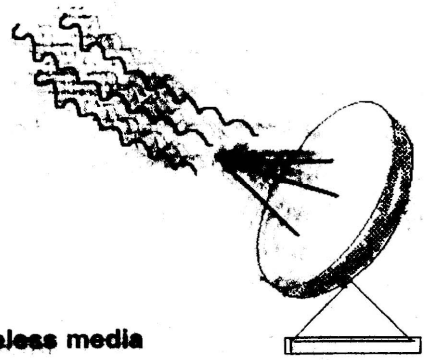
  A mobile machine connects to the home network using cellular or satellite technology.

Wireless networks are especially useful in the following situations :

1. Spaces where cabling would be impossible or incontinent. These includes open lobbies, inaccessible parts of buildings, older buildings, historical buildings where renovation is prohibited, and outdoor installations.
2. People who move around a lot within their work environment Network administrators, for instance, must trouble shoot a large office networks.
3. Temporary installations. These situations include any temporary department set up for a specific purpose that soon will be torn down or relocated.
4. People who travel outside of the work environment and need instantaneous access to to network resources.

Wireless media transmits and receives EM (electromagnetic signals without an electrical or optical conductor. Thus earth's atmosphere provides the physical data path for most wireless transmissions. Followings are some transmission medias, which normally used for wireless transmissions.

- Radio wave
- Microwave
- Infrared light



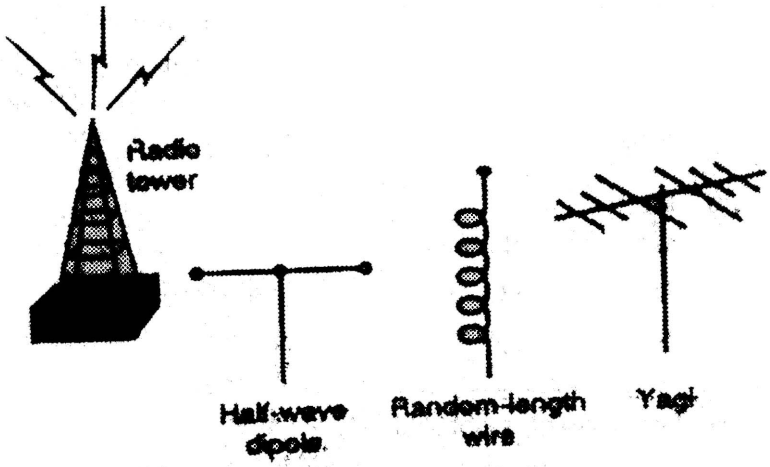
Wireless media

3.4.1 Radio frequency

The portion of EM spectrum between 10KHz- 1 GHz is considered as radio frequency (RE) this range of radio frequencies includes broadcast bands commonly called as

- Short-wave (SW) radio
- Very high frequency (VHP) television and FM radio.
- Ultra-High frequency (UHF) radio and TV

Radio frequencies have divided between regulated and unregulated. Users of regulated frequencies must get a license from the regulatory bodies. Error-free transmissions are impossible to guarantee in uncontrolled frequency bands. Following are the typical radio frequency equipments:



Typical radio frequency equipments

Typical radio frequency equipment

Radio frequency waves can be broadcast in all directions. Typical antennas include omni directional towers, random length wire, half wave dipole and beam (such as yagi). Global systems use short wave, which propagates beyond the horizon and local systems are use nearly line-of-sight VHF or UHF.

Frequency range

Radio frequency operates within the entree RF range. Computer networks typically use the higher GHz ranges because they offer higher transmission rates.

Cost

Depending upon the combination of transceiver and antenna used, radio frequency systems are moderately priced compared to other wireless media.

Ease of installation

Ease of installation is also dependant upon the combination of transceiver and antenna used. Most systems are easily installed with pre-configured antenna and other equipment. Low power single-frequency systems are simple to install compared to high-power, single frequency systems.

Bandwidth

Single frequency radio systems offer transmission rate ranging from 1 Mbps to 10*Mbps.* Spread spectrum radio which uses multiple frequencies simultaneously) offer transmission rates ranging from 2 to 6 Mbps.

Attenuation

Attenuation of all RF ranges are dependent upon frequency and power of the signal. Because low-power, single frequency devices normally operate at very low power, they usually suffer from relatively high attenuation. The, high power, single frequency devices sustain the signal and resist attenuation much better that low-power devices.

Immunity from EMI

Single frequency signals have extremely low immunity from EMI, compared to spread spectrum. Spread spectrum resists eavesdropping.

Advantages

- No intervening ground facilities are required between stations.

- Directional equipment is not needed.
- Stations can be stationary or mobile; even on aircraft or marine vessels.
- Radio is accessible to users thought the world
- Radio transceivers are inexpensive.

Disadvantages

- AH RF transmission devices may require frequency licensing.
- Only low bandwidths are offered (between 1 Mbps to 10 Mbps)
- Highly susceptible to external interference and jamming.
- Except spread spectrum radio, al single-frequency radio devices are susceptible to eavesdropping.

3.4.2 Microwave

Microwave data communication system is' exit in two forms:

- Terrestrial (earth-based) systems
- Satellite systems

Functionally both terrestrial and satellite systems use the same frequencies (in the range of 1 GHz to 300 GHz) and are similar, but the capabilities of each are somewhat different.

Terrestrial (earth-based) systems

Terrestrial, microwave typically uses directional parabolic antennas that require an unobstructed |^|h or line-of-sight to other units. Terrestrial microwave signals, commonly in the low GHz frequency ranged are generated by a transceiver. Terrestrial microwave links are often used to link separate buildings where cable installation would be troublesome or more expensive, Smaller scale terrestrial microwave may also be used within buildings.

Frequency range

Terrestrial microwave system usually operate in the low GHz range, typically between 4 to 6-GHz and 21 to 23 GHz

Costs

Equipment costs are most dependant upon the operating signal strength and frequency. Short-distance systems, used within hundreds of meters of .distance, are relatively inexpensive. Long-distance systems, used at kilometers of distance, may be quite expensive. Terrestrial microwave systems may be leased from service providers to reduce the initial fixed costs.

Ease of installation

Line-of sight systems are difficult to install because they require very exacting adjustments often made by trial error, to ensur proper alignment. Since Terrestrial microwaves typically operate in licensed frequencies, installations, require expensive and time-consuming licensing procedures.

Bandwidth

Typical data rates for a single-frequency range between 1 to 10 Mbps.

Attenuation

Attenuation varies with the signal frequency and antenna size. Higher

frequency microwaves are attached more by rain and fog over long distances, but across short distances attenuation is not much.

Immunity from EMI

Microwave links are susceptible to external interference, jamming, and eavesdropping.

Advantages

- Potentially much less expensive than digging trenches etc.
- High bandwidths are possible

Disadvantages

- Require government licensing and approved equipment
- Susceptible to external interference, jamming and eavesdropping
- Installation is complex when direct line-of-sight is not available

Satellite microwave

Like Terrestrial microwave, satellite microwave systems use low GHz frequency range microwaves. However, they are beamed line-of-sight between directional parabolic antennas located on earth and geo-synchronous orbiting satellites. A basic satellite network installation includes a network connectivity device called VSAT (very small Aperture Terminal), which is attached to a parabolic antenna (popularly known as satellite disk) of 2-meter diameter approximately, by means of cable media. The dish antenna reflects signals generated by transponder to a satellite.

The beauty of satellite microwave communication is that it requires the same time and expense whether two VSAT station are away from each other, 10 or 10000 kilometers. In case of one top transmission a signal has to travel about 72000 kilometers of distance. While in case of two hop transmission, a signal has to travel about 1,44,000 kilometers of distance. Due to this long travel in space satellite transmissions are subject to propagation delay of how a second to 5 seconds. However they can provide a signal to the most remote and undeveloped areas on the globe.

Advantages

- Propagation delay and communication cost are independent of distance between sending and receiving stations.
- High bandwidths possible
- No intervening ground facilities are require between transmission points even between continents.
- Earth stations can be fixed positions or relatively mobile, even on aircraft or marine vessels.
- Satellite communication supports narrow or wide beam paths, so transmission can be relatively selected or broad-based.

Disadvantages

- Susceptible to external interference, jamming, and eavesdropping.
- Require high precision. Complex equipments cost can be reduced by hiring services from satellite service providers.
- Propagation delay of 1 to 5 seconds
- Apart from one time installation cost, organizations may have to very high annual operation charges to the satellite service providers.

Check your progress - 3.4.1 & 3.4.2

1. What is wireless media?

   ……

   ……

2. Explain the advantages and disadvantages of satellite transmission?

   ……

   ……

3. What is a frequency range for Terrestrial system?

   ……

   ……

4. Explain the following characteristics of radio frequency waves?

   Frequency range……

   Bandwidth……

   Attenuation……

3.4.3 Infrared Light

Infrared links are light emitting diodes (LEDs) or Injection laser diodes (ILDs) and photodiodes to exchange data between stations. Infrared signals -are not capable of penetrating walls or other opaque objects and are diluted by strong light.

This system will fail in two categories

1. Point to point
2. Broadcast

Point to point

Because infrared waves may be cheaply and easily Segregated, pure beams may be focused tightly and directed at specific targets. This strategy reduces the effects of attenuation and possibility of eavesdropping. Remote control device to operate TV is file best example of point-to-point infrared system:

Advantages

- Mass production makes interface relatively
- High transmission rates possible, but current technology support bandwidth up to 16Mbps.
- Resists eavesdropping.

Disadvantages

- Requires strict line-of-sight paths and exact positioning.
- Susceptible to high intensity light and atmospheric conditions.

Broadcast Infrared systems

A broadcast infrared system relaxes the focus of the beam to broadcast or diffuse the signal to span a wide area. This method is also commonly used with remote controls and other user devices. It is much easier to line up transceivers using this technique and receiving devices have much more flexibility to move around. One transceiver may communicate with multiple.

Advantages

- Mass manufacturing makes some interface devices relatively inexpensive
- Does not require exact positioning and is ideal for locally mobile devices

Disadvantages

- Lower transmission rates than point to point infrared systems.
- Susceptible to high intensity light and atmospheric conditions.
- Highly susceptible to eavesdropping.

3.5 SUMMARY

Computer use electronic voltage pulses or electromagnetic waves to send signals. The physical path through which the electrical voltages and EM waves travel is called Transmission Media. Transmission media can be classified as cable (bounded) or wireless (unbounded).

In FDM this technique works by converting all data channels to analog form. Each analog signal can be modulated by a separate frequency (called a carrier frequency) that makes it possible to recover that signal during demultiplexing process.. FDM can be used in broadband LANs

In TDM it divides a channel into time slots that are allocated to the data streams to be transmitted. If the sender and receiver agree on the time-slot assignments, the receiver can easily recover and reconstruct the original data streams; Time Division Multiplexing transmits TDM the multiplexed signals in baseband mode.

In this we also studied different type of cables are used as a transmission media

- Coaxial Cable
- Twisted-pair
- Fiber optic cable

Source : *www.scribd.com(Link)*

3.6 CHECK YOUR PROGRESS – ANSWERS

3.1 – 3.2

1. The physical path through which the electrical voltages and EM waves travel is called Transmission Media. Or transmission media make possible the transmission of the electronic signals from one computer to another computer.
2. Each type of transmission media has special characteristics that make it suitable for a specific type of service.
    - capacity (bandwidth)
    - Ease of installation
    - Attenuation
    - Immunity from electromagnetic interference (EMI)
    - Cost
3. Time Division Multiplexing divides a channel into time slots that are allocated to the data streams to be transmitted. If the sender and receiver agree oh the time-slot assignments, the receiver can easily recover and reconstruct the original

data streams. Time Division Multiplexing transmits the multiplexed signals in baseband mode.

4. Attenuation is a measure of how much a signal weakens as it travels through a medium. ;

5. Transmission media make possible the transmission of the electronic signals from one computer to another computer. Through transmission media networked computer signals each other. Computer networks relay upon the ability of transmission medium to accommodate a range of electric voltage or EM waves.

6. Electromagnetic interference consists of outside electromagnetic noise that distorts the signal in medium.

3.3.1

1. Difference between broadband and baseband coaxial cable-: Baseband is thin, light and flexible cabling medium,; which is inexpensive and easy to install. Broadband cables are thicker in diameter and harder to work with. This carries more signals for greater distance then baseband cables. Because of its greater size, it is also more expensive than baseband cable. It can be installed safely outside, running from building to building.

2. The components of the co-axial cable are as follows-:

- A central conductor, Although usually solid copper wire, this sometimes is made of standard, wire
- An outer conductor forms a tube surrounding the central conductor. This conductor can consist of braided wires, metallic foil or both. The outer conductor, frequency called the shield, servers as a ground and also protects the inner conductor from EMI.
- An insulation layer keeps the outer conductor spaced evenly from the inner conductor.
- A plastic encasement (jacket) protects the cable from damage.

3. Two types of connectors are commonly used with coaxial cable. The most common is the BNC connector mainly used for thinnet cabling. In contrast thicknet uses N-Connectors, which screw on instead of using a twist lock.

3.3.2

Capacity of UTP cables - The data rates possible with UTP have increase from 1 Mbps; pat 4 and 16 Mbps, to the point where 100 Mbps data rate age now common.

Capacity of STP cables-: STP cable has a theoretical capacity of 500 Mbps, although few implementations exceed 155 Mbps with 100 meters cable runs. .The most common data rate for STP cable is 16 Mbps, which is the top data rate for Token Ring networks.

2. Advantages of UTP cable

- Relatively inexpensive
- Easily installed, managed, and reconfigured
- Basic technology and standards are matured and stable

3.3.3

1. Loose configuration incorporates a space between the fiber sheath and the outer plastic encasement; this space is filled with gel or other material. Whereas |n

Tight configuration contains strength, wires between the conductor and the outer plastic encasement.

2. Advantages of fiber optic cable-:

- Supports very high bandwidth - from 100 Mbps to > 2Gbps
- Very low attenuation
- Immune to BMI or eavesdropping

Disadvantages

- Very expensive cables
- More complex to install
- High precision required for connections

3.4.3 & 3.4.2

1. People who need to be online all the time, for these mobile users twisted pair co-axial cable are of no use. For them networks are developed without cables are called as wireless media. It transmits and receives EM signals without an electrical or optical conductor. Earth's atmosphere provides the physical data path for most wireless transmission.

2. Advantages of satellite transmission

- Propagation delay and communication cost are independent of distance between sending and receiving stations
- High bandwidths possible
- No intervening ground facilities are require between transmission points even between continents.
- Earth stations can be fixed positions or relatively mobile, even on aircraft or marine vessels.
- Satellite communication supports narrow or wide beam paths, so transmission can be relatively select or broad-based.

Disadvantages

- Susceptible to external interference, jamming and eavesdropping.
- Require high precision. Complex equipments cost can be reduced by hiring services from satellite service providers.
- Propagation delay of 1 to 5 seconds

3. Terrestrial microwave system usually operates in the low GHz range, typically between 4 to 6 GH and 2t to 23 GHz.

4. Characteristics for radio-frequency waves

- **Frequency range-:** Radio frequency operates within the entice RF range. Computer networks typically use the higher GHz ranges because they offer higher transmission rates.
- **Bandwidth -:** Single frequency radio systems offer transmission rate ranging from 1 Mbps to 1 0 Mbps Spread spectrum radio (which uses multiple frequencies simultaneously) offer transmission rates ranging
- **Attenuation-:** Attenuation of all RF ranges are dependent upon frequency and power of the signal. Because low-power, single frequency devices normally operate at very low power, they usually suffer from relatively high attenuation. The high power, single-frequency devices sustain the signal and resist attenuation much better that low-power devices.

3.7 QUESTIONS FOR SELF – STUDY

1. Define computer networking transmission media?
2. Explain attenuation?
3. What is distance limit for UTP cables?
4. Write note on
    - EMI for transmission
    - Fiber optic cable
    - Coaxial cables
    - Wireless media
5. Explain TDM and FDM with Help of figure?
6. Differentiate between STP and UTP cables?
7. Explain co-axial cable with their characteristics?
8.. How bandwidth affects to transmission media?
9. Explain the advantages of twisted pair cable?
10. Write note satellite communication?

3.8 SUGGESTED READINGS

1. Computer Networks : Andrew Tanenbaum
2. Cisco CCNA Certification Guide : Wendell Odom

❁❁❁

Chapter 4

Network Connectivity Devices

4.0 OBJECTIVES

After studying this chapter you will be able to-

- State different network connectivity devices
- Discribe to devices like modem, brouters, routers, bridges, switches etc.

4.1 INTRODUCTION

In this chapter OSI module provide set of standard rules for networking.

Model contains 7 layers, each layer performs different task. The first layer is physical layer. It uses the bit and signals to communicate. The second layer is data link layer. It is responsible for the creation and interpretation of different frame types based on a actual physical network being used. The Network layer is third layer and is mostly associated with the movement of data by means of addressing and routing. The fourth layer is the transport layer, it is primarily responsible for guaranteeing of packet transmitted by the network layer. Session layer is the fifth layer, it is responsible for managing connecting between two machines during the course of communication between them. Presentation layer is primarily concerned with the conversion of data formats, in the form of packets, from one machine to another. The seventh layer of the OSI model is application layer. It acts as the arbiter or translator between user's applications and the network.

The interfaces and devices that are used to connect computing devices and transmission media are called connectivity hardware or network connecting devices. Network connectivity hardware connects individual devices to a single network, for eg a pc or printer would use network connectively devices to connect to UTP or some other that we are going to study in particular section of your book.

4.2 OSI MODULE - AT A GLANCE

Now all of you are aware of what networking, transmission media and cable media that we can use to transmit data from one terminal to other terminal For understanding process of data transmission there are some standard rules. In previous year you already studied OSI module, that module provides standard rules for networking.

Layer	Purpose
Application	Interface to network services
Presentation	Translates between Application and others, redirector, encryption, compression.
Session	Establishes rules for communication, determines synchronisation
Transport	Handles network transmission
Network	Addressing, traffic, switching
Data Link	Error checking, manages link control, communication with cards
Physical	Network interface card, wire, and so on.

1. Physical layer

The first layer is the physical layer. It uses the bits and signals to communicate.

This is the only layer that is truly connected to the network in the sense that it is the only layer concerned with how to interpret the voltage on the wire- the 1s and Os. This layer is responsible for understanding the electrical rules associated with devices and for determining what kind of medium is actually being used (cables, wires, connectors, and other mechanical distinctions.)

It is important to note that while the OSI model doesn't define the media used, the physical layer is concerned with all aspects with all aspects of transmitting and receiving bits on the network.

2. Data link Layer

The second layer is data link layer. It is responsible for the creation and interpretation of different frame types based on the actual physical network being used. This layer is also responsible for interpreting what it receives from the physical layer. Using low – level error detection and correction algorithms to determine when information needs to be re-sent. Network protocols including the TCP /IP protocol suite, don't define physical standards at the physical or data-link layer, but instead are written to make use of any standards that may currently be in use.

3. The Network layer

The third layer of OSI model is the Network layer. It is mostly associated with the movement of data by moans of addressing and routing. It directs the flow of data from a source to a destination, despite the fact that the machine might not be connected to the same physical wire or segment, by finding a path or route from a machine to another. It is necessary; this layer can break data into smaller chunks for transmission. This is sometimes necessary while transferring data from one type of physical network to another network. This layer is also responsible for reassembling those smaller into the original data after the data has reach edits destination.

To restate : The network layer involves communication with devices on logically separate networks connected to form internet works can be large and can be constructed of different types of networks, the network layer utilizes routing algorithms that can be used to guide packets from their source to their destination network.

A key element of the network layer is that each network in the internetwork is assigned a network address and they are used to route packets constitute the topics of address and switching.

4. The Transport layer

The fourth layer is the transport layer. It is primarily responsible for guaranteeing delivery of packets transmitted by the network layer, although it doesn't always have to do so. Depending on the protocol being used, delivery of the packets may or may not be guaranteed. When the transport layer is responsible for guaranteeing the delivery of packets, it does so through various means of error control, including verification of sequence members for packets and other-protocol-dependant mechanism.

5. The session layer

The fifth layer is session layer-it is responsible for managing connections between two machines during the course of communication between- them. This layer determines whether it has received all information for the session and whether it can stop receiving or transmitting data packets. This layer also has built-in error correction and recovery methods.

6. The presentation layer

The sixth layer Is the Presentation layer. it is primarily concerned with the conversion of data formats, in the form of packets, from one, machine to another. One common example is the sending of data from a machine that uses the ASCII format for characters to a, machine that uses the, EBCDIC format for characters, typically of IBM mainframes.

The presentation layer is responsible for picking up differences such as these and translating them to compatible formats. Both EBCDIC and ASCII are standards for translating characters to hexadecimal code. Letters, numbers; and symbols in one format which must be translated when communicating with machines using a different format. This is the responsibility of the presentation layer.

7. The Application layer

The seventh layer of the QSI model is the application layer. It acts as the arbiter or translator between user's application and the network. Applications that want to utilise the network to transfer messages must be written to conform to networking APIs supported by machine’s networking components, such as windows sockets and NetBIOS. After the application makes an API call, the application layer determines which machine it wants to communicate with, whether a session should be set up between the communicating machines, and whether the delivery pf packets needs to be guaranteed.

Benefit of OSI layered Architecture

Many benefits can be gained from the process of breaking up the functions or tasks of Networking into smaller chunks, called layers, and defining standard interfaces between these layers, The following list summarises the benefits of OSI Layered architecture:

- The individual protocols or layers are less complex and therefore can be defined in great detail.
- Reduced complexity allows easier program changes and faster product evolution.
- It facilitates systematic troubleshooting.
- You can change one layer without having to change all layers.
- It helps divide complex network operation into more manageable layers.

- A better environment for interoperability is created.
- One layer uses services of the layer immediately below it. Therefore, remembering what each layer dose is easier.
- It helps design the standard interface for the " plug-and-play" multi-vendor integration.
- It clarifies what general function is to be done father how to do it.

Interaction between OSI Layers

The process of how the layers interact on the same computer, as well as how the same layer processes on different computers communicate with each other, is all interrelated. The software or hardware products implementing the logic of some of the OSI protocol layers provide two general functions:

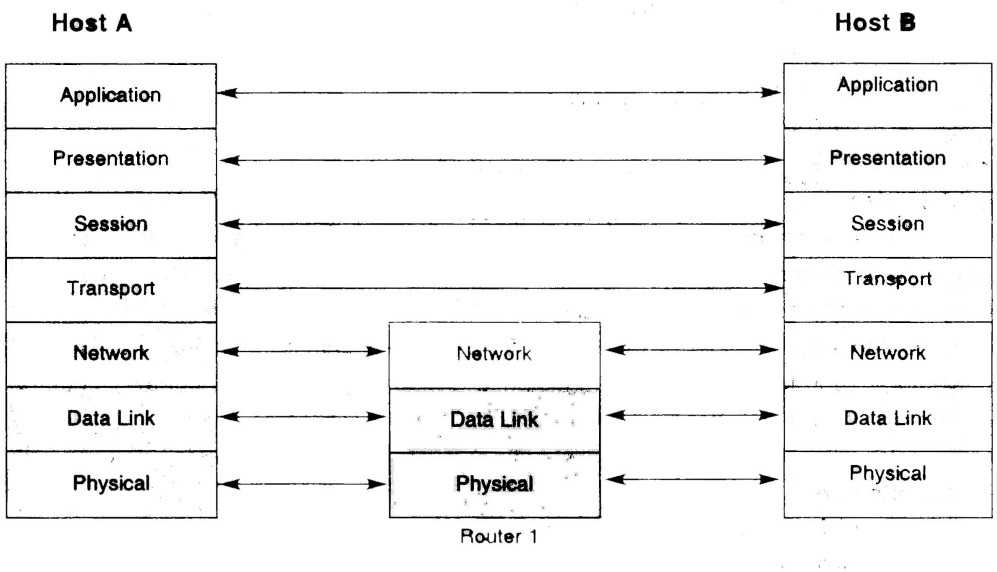
- Each layer provides a service to the letter above it in the protocol specification.
- Each layer communicates some information with the same layer's software or hardware on cither computers.

Interactions between Adjacent layers on the same Computers

To provide services to the next higher layer, a layer must know about standard interfaced defined between layers. These interfaces include definitions of what Layer N +1 must provide 10 Layer N to get services, as well as what information Layer- N must provide back to N+1.

The figure presents a graphical representation of two computers and provides an excellent means of interaction between layers on the same computer.

The data is cheated by some application on Host A. for, example; the user types an e-mail message. Each layer creates a header and passes the data down to the next layer.



Passing the data down to the next layer implies that the lower needs to perform some services for the higher layer. To perform these services, the lower layer adds some information in a header or trailer. For example, the transport layer hands over its data and header to the network layer. The network layer adds header with the correct destination network layer address so that the packet can be delivered to the other computer.

From each layer's perspective, the bits after that layer's header are considered to be data. For example, Layer 4 considers the Layer 5, 6, and 7 headers, along with original user data, to be one large data field.

After the application creates data, the software and hardware implementing each layer perform their work, adding the appropriate leader and trailer. The physical layer can use the media to send a signal for physical transmission as shown in step 2.

Upon receipt (step 3) Host B begins the adjacent layer interactions on host-B. The right side of above figure shows an arrow pointing next to the computer (step 4) signifying that the received data is being processed as it goes up the protocol stack. The following sequence outlines of basics of processing at each layer and shows how each lower layer provides a Service to the next higher layer. Consider the receipt of data by the host Son right side of the figure.

Step 1- The physical layer ensures bit synchronisation and places the received finery pattern into the buffer. It notifies the data link layer that a frame has been received after decoding the incoming signal into a bit stream. Thus physical layer has provided delivery of a stream of bits across the medium.

Step 2- The data link layer examines the frame check sequence (PCS) in the trailer to determine whether errors occurred in transmission (error detection). If an error has occurred, the frame is discarded. 'The data link addresses are examined so that host B can decide whether to process the data further. If the data is addressed to host B, the data between the layer 2 header and trailer, is given to the layer 3 software. Layer 2 has delivered the data across that link.

Step 3- The network layer destination address is examined. If the address is host B's address, processing continues and the data, after the layer-3 header, is given to the transport layer software. Layer 3 is provided a service of end-to-end delivery.

Step-4- If error recovery was an option chosen for the transport layer, the counters identifying this piece of; data .are encoded in the layer-4 header along with acknowledgement information (error recovery). After error recovery and reordering of the incoming data, the data is given to the session layer.

Step 5- The session layer can be used to ensure that a series of messages is completed. After the session layer ensures that all flows are completed, it passes the data, after the layer-5 header, to the layer-6 software.

Step 6- The presentation layer defines and manipulates data formats. For example, if the data is binary instead of character data, the header denotes that fact. The receiver does not attempt to convert the data using the default ASCII character set of host B after the data formats have been converted, the data, after the Layer-6 header, is then passed to the Layer-7 software.

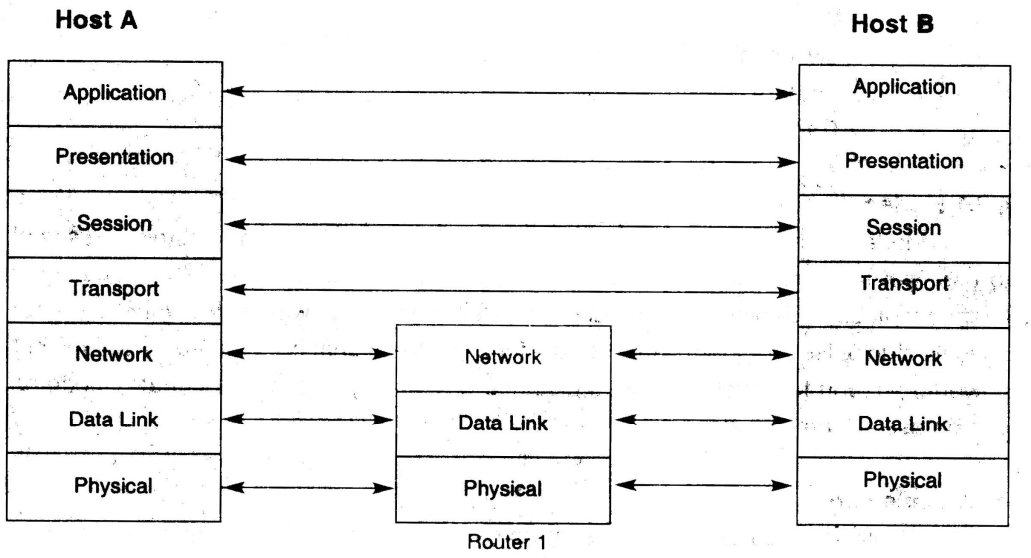
Step 7- The application layer processes the final header and then can examine the true end-user data. This header signifies agreement to operating parameters by the application on Host A and Host B. The Reader typically is sent and received at application initialization time only. For example, for file transfer, the size of the file to be transferred and the file formats used would be communicated (application parameters) at the initialization time.

Interactions between the tame layers on different computers

Layer N (where N*1 to 7) must interact with layer N on another computer to successfully implement its functions. For example, the transport layer»can send data but if another computer does not acknowledge that the data was received, the sender will not know when to perform error recovery.

To interact with the same layer on another computer, each layer defines a header, arid, in some cases, a trailer. Headers, and trailers are additional data bits, created by the sending computer's software or hardware, that are placed before or after the data given to Layer N by Layer N+1- The information needed for this layer to

communicate with the same later process on the other computer is encoded in the header ands trailer. The receiving computer's Layer N software or, hardware interprets the headers and trailers created by the sending computer's layer N, learning how Layer N's processing is being handled.



The application layer on host. A communicates with the applications layer on host B. likewise the bottom three layers of tie OSI model haw to do with delivery of data. Router 1 is involved that process. Host A's network, data link and physical layers communicate with likewise router 1 communicates with Host B's physical,

4.3 NETWORK COWNECTIVITY DEVICES

The interfaces and devises that are used to connect computing devices and transmission media are called connectivity hardware or network connectivity devices.

Network connectivity hardware connects individual devices and transmission media are called connectivity hardware or network connectivity devices".

Network connectivity hardware connects individual devices to a single network, for example a PC or printer would use network connectivity devices to connect to UTP or some other that we are going to study in particular section of your book.

- Modern
- Repeaters
- Hubs
- Bridges
- Multiplexes
- Switches
- Routers
- Transmission media connectors etc.

4.3.1 Modem (modulator/ demodulator)

Modem converts your computer digital signal to an analog transmission signal to use with telephone tines or microwave transceivers. Modem is necessary because telephone lines and microwave media uses electromagnetic waves, but your computer uses electric pulses. Modems are also useful when the signal from the transceiver is hot powerful enough to travel a required, distance without significant loss of data, modems can be used to amplify signals.

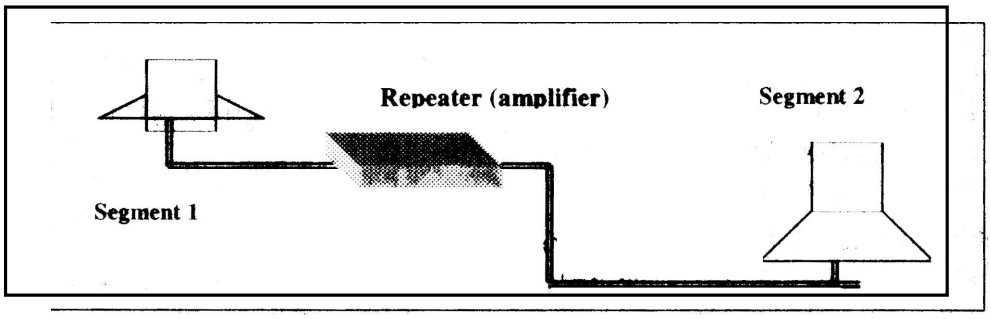
4.3.2 Repeaters

When an electrical signal is sent across a medium, It fades along the distance (known as attenuation) as a result of resistance from the medium itself. Naturally the

longer the distance that it travelled, the more the signal fades. Eventually tie signal fades to a, point where the receiving station cannot recognise the original message (Or has trouble doing so).

In short each transmission medium can be used for a certain distance. However you can exceed the physical medium's maximum effective distance by using an amplification, device called as Repeater. It works at OSI physical layer. A repeater operas at the physical layer of the OSI model and takes a signal from one LAN and sends it to another LAN- reconditioning and retiming it in the process. The reconditioning usually amplifies and boosts the signal's power. If the signal has travelled a distance it is weak, and so on, the amplification can also be done on noise receivers.

The repeaters job is simple: it detects the signal, amplifies and retimes it, and sends it through all the ports except the one on which the signal was seen. It is important to note that since the repeater has no real knowledge of the data it is carrying, no error checking is performed. Therefore any error are passed from one segment to the next without any ability to stop it. Many networks limit the number of repeaters between the transmitting and receiving stations. On other side, by not performing any filtering, the -repeater does not slow down the network's speed or performance. The signal has travelled a distance is weak, and so on, the amplification can also be done on noise received.



Pros and Cons of repeaters

Pros	Cons
Allow you to extend the network over large distances.	Have no knowledge of addressing or data types.
Do not affect the speed of network	Can't ease network congestion problems
Can connect network segments of different media.	Limit the number of repeaters that can be used.

Check your Progress - 4.3.1 – 4.3.2

1. Explain the purpose of Application layer?

   ……

   ……

2 Define network connectivity devices?

   ……

   ……

3. What is use of Repeater?

   ……

   ……

4.3.3 Hubs

In order to connect various cable segments, we need a central point to plug every thing together. A hub is-a multiport repeater. It provides point-to-multipoint connections, it is basically a shared device and works at physical layer of the OSI model. It is often located in a wiring closet and is a point of concentration for wiring.

There are three types of hube namely,

- Passive hub
- Active hub
- Intelligent hub

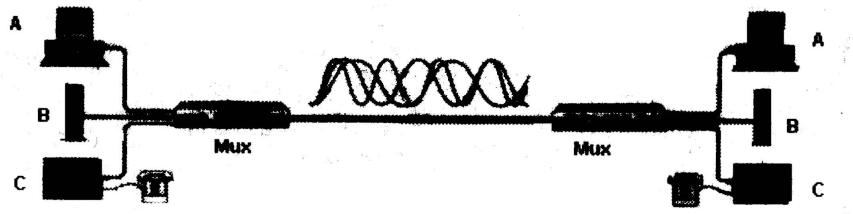
A passive hub connects cable segment together. No signal regeneration is performed. So each segment is allowed to be extended to only half the maximum effective distance.

An active hub is like a passive hub except it regenerates or amplifies signals. The main drawback of active hub is that some active hubs amplify cable noise as well as signal.

An intelligent hub, in addition to signal regeneration, also helps in performing network management functions. The SNMP (simple network management protocol) agents must be embedded in a hub to carry out network related functions.

4.3.4 Multiplexers

Multiplexer combines two or more separate signals onto one high-speed transmission media. It is also known as mux, and is often used to allow remote terminals to communicate with front-end processor ports over a single line. It works at OSI physical layer.



4.3.5 Bridges

Bridges connects two separate networks to form a logical one by operating at the data link layer of the OSI model. Bridges rely on MAC addresses for their operation. Unlike repeaters, bridges examine the packet's destination address before forwarding it to other segments. A bridge extends the maximum distance of your network by connecting separate network segments, and selectively pass signals from one medium segment to another.

Bridges isolate the media access mechanisms of the LANs to which they are connected. If a packet has a destination address on the same network segment as the source of the signal, the bridge ignore the signal. If the destination address is different from the source address network segment, the bridge sends the message along in a fashion similar to what a repeater would. Since bridges are selective about which data packets can be transferred, they are useful in solving traffic bottlenecks it must be noted, however that bridges do not reduce traffic caused by broadcast packets or broadcast storms.

Although they are effective for a small number of LANs, bridges lose many of their benefits as the number of LANs grows. Bridges only operates at the data link layer, and the best source routing information is a component of the network layer.

Bridges offer following advantages over hubs :

1. Divide a large network segment into smaller segments and hence reduce data traffic and improves network performance.

2. Filter local data traffic by not allowing them to cross other network segments hence reducing overall network traffic.

3. Provide exclusive bandwidth (10 Mbps) to each node connected to a port on a bridge as opposed to shared bandwidth provided by hubs.

4. Can be used to connect network segments of dissimilar media.

Pro	Cons
Can act as a repeater and extend distance	Slower than repeaters due to the need to examine addresses
Easy to install, load, and configure	Can't perform effective balancing on larger networks
Can restrict flow and ease congestion	More expensive than repeaters
Useful for protocols that can't be routed	Can’t prevent broadcast storms
Have good cost – to – performance ration	Certain application might not run on bridge networks.

4.3.6 Switches

As a response growing network demands, devices known as switches were introduced to the market in 1991. A switch is a big brother of bridge. The switch is nothing but a large multiport bridge. The switch operates at layer 2 of the OSI model just like a bridge that MAC addresses to determine where to forward the packet. The main differences between switches and bridges, are the strength and speed offered by the switches. Bridges can have maximum 16 ports while switches can offer hundreds of ports, each port offering exclusive bandwidth of 10 or 100 Mbps.

Switches can perform following functions.

- Address learning.
- Filtering and forwarding
- Loop Avoidance

Check your progress. - 4.3.3 to 4.3.6

1. What is use of Hub?

   ……

   ……

2. Bridges are acting on which layer of OS) model?

   ……

   ……

3. What are the advantages of bridge?

   ……

   ……

4.3.7 Routers

Routers are the most complicated of the three devices so far, operating at the network layer of the OSI model. While bridges are limited to examine data packets MAC addresses, routers go beyond this and-can examine the network address-which has routing information encoded in it. Routers can use this information to make

intelligent decisions about routes and paths.

In the simplest form routers like bridges-can be used to connect network segments. Whereas bridges only know to forward what they don't recognised, routers are aware of multiple paths that lead to a destination address and know which path is best.

Each network segment is assigned a specific address and is then referred to as a sub network or subnet. Each node on the network is then assigned an address. Every data packet sent contains the destination network address and node address. The optimum path can then be determined by looking at infernal routing table.

One of the biggest differences Between brides and routers is the ability to identify where data is going, the router must initialize and maintain the routing table and determine the next hop in the packet's journey, a router is expected to be able to identify the address and only send packets for which it has a network address. If a machine address isn't found in the routing table, the packet is discarded.

To get at the network layer and find the information it needs, the router must first strip off the Data Link Layer. After it finds the information, it repackages the data packets. A key advantage of routers comes into play during this operation: Since the data is unpacked and repacked, there wan opportunity transform the data to the data frame needed for a particular architecture.

Routers are normally responsible for performing the following functions :

- **Route selection -**

  A router is maintaining the information in its routing table about how to reach remote networks. It will then make routing decisions based on that information

- **Logical addressing-**

  A device that operates at layer 3 requires some form of logical addressing. These addresses will be used to determine route selection.

- **Segmentation-**

  routers can be provide by a powerful method of segmenting your networks to allow optimum utilization of available bandwidth.

Advantages of using Routers

- **No broadcasts**

  Because router operates at Layer 3 of the OSI mode), no Layer 2 broadcasts wiII be forwarded through a router.

- **Manageability**

  Routers have a better knowledge of the network topology than bridges and switches do and have the ability to support more protocols than bridges and switches

- **Increased bandwidth**

  By segmenting your networks with routers, your nodes/ hosts will have more access bandwidth

- **Packet fragmentation and reassembling**

  Routers provide, packet fragmentation / reassembly functions, as well as better Security.

Pros	Cons
Can perform more functions than bridges	Considerably more difficult to install than Bridge
Can interconnect network segments of differing architectures.	More expensive than repeaters or bridges

Can manage load balancing and sharing	Work only with routable protocols
Can be used to control broadcast storms	Static routing can cause problems
Can choose the best path and make dynamic changes	Much slower than bridges or repeaters due to additional functions.

4.3.8 Brouters

Bridges can perform limited functions but can work with all protocols. Routers on the other hand, perform more complex functions but can work with only certain protocols. Brouters come into play as a combination of the best features of the two. If a routable packet is received, the brouter routes the data to the appropriate destination. If a no routable protocol sends data, however the brouter bridges the data based on the hardware address. In order to perform both functions, the brouter must contain both a routing table and a bridging table. As a result it operates at both the Network arid Data Link Layer. Brouters are more expensive and complex than bridges and routers.

4.3.9 Gateways

Gateways are often lumped into discussion about bridging and routing, when in fact the-service they perform is similar but different by one major factor: with a gateway, data is translated between two different data formats or network architectures.

Gateways perform much higher-level translations than any other component and thus work at the Application layer of the OSI module. When packets arrive at a gateway, all the information is stripped off the data until it reaches the layer where it can translate the information-using the format needed for the destination

Pros	Cons
Can connect completely different systems.	Very expensive than other devices.
Specialize in one task only	Difficult to install and configure. Depending oh the level of translation, can be very slow

4.4 SUMMARY

In this chapter we have studied OSI module that provides set of standard rules for networking. Model contains 7 layers each layer performs different task.

The first layer is the physical layer. It uses the bits and signals to communicate. This is the only layer that is truly connected to the network in the sense that it is the only layer concerned with how to interpret the voltage on the wire the 1s and 0s. This layer is responsible for understanding the electrical rules associated with devices and for determining what king of medium is actually being used.

The second layer is data link layer. It is responsible for the creation and interpretation of different frame types based on the actual physical network being used. This layer is also responsible for interpreting what it receives from the physical layer. Using low-level error detection and correction algorithms to determine when information needs to be re-sent.

Network layer is mostly associated with the movement of data by means of addressing and routing. It directs the flow of data from a source to a destination,

despite the fact that the machine might not be connected to the same physical wire or segment, by finding a path or route from one machine to another.

The fourth layer is the transport layer. It is primarily responsible for guaranteeing delivery of packets transmitted by the network layer, although it doesn't always have to do so. Depending on the protocol being used, delivery of the packets may or may not be guaranteed. When the transport layer is responsible for guaranting the delivery of packets, it does so through various means of error control, including verification of sequence members for packets and the/ protocol dependant mechanism.

The fifth layer is session layer it is responsible for managing connections between two machines during the course of communication between them.

Presentation layer is primarily concerned with the conversion of data formats, in the form of packets, from one machine to another.

The seventh layer of the Oil model is the application layer. It acts as the arbiter or translator between user's applications and the network.

4.5 CHECK YOUR PROGRESS – ANSWERS

4.3.1 & 4.3.2

1. **Main purpose of Application layer-** The layer acts as the arbiter or translator between user's applications and the network. The application layer determines which machine it wants to communicate with, whether a session should be set up between the communicating machines, and whether the delivery of packets needs to be guaranteed.
2. **The interfaces and devices that are-** used to connect computing devices and transmission media are called connectivity hardware or network connectivity devices.
3. When an electrical signal is sent across a medium, it fades along the distance. Each transmission medium can be used-for a certain distance. But with use of repeaters you can exceed the physical medium's maximum effective distance. Repeaters amplify and retimes the signal.

4.3.3 & 4.3.5

1. A hub is a multiport repeater. It provided point-to-multipoint connections. There are three types of hubs namely,

- Passive hub
- Active hub
- Intelligent hub

2. Bridges always acts on OSI-Data Link Layer.

3. Bridges offer following advantages over hubs.

1. Divide a large network segment into smaller segments and hence reduce data traffic and improves network performance.

2 Filter local data traffic by not allowing them to cross other network segments hence reducing overall network traffic.

3. Provide exclusive bandwidth (10 Mbps) to each node connected to a port on a bridge as opposed to shared bandwidth provided by hubs.

4. Can be used to connect network segments of dissimilar media.

4.6 QUESTIONS FOR SELF – STUDY

1. Define connective hardware?
2. Which of the following connectors are used with UTP media?
   - BNC
   - RJ-25
   - D-4
   - RJ-45
3. Which of the following media connector devices converts computer's digital signals to analog signals?
   - Transceiver
   - LAN card
   - Modem
   - All of the above
4. Explain the use of repeaters?
5. What are bridges and what are the advantages of bridge over hub?
6. What are advantages of routers?
7. Write note on purpose of physical and network layer of QSJ model?
8. What are the benefits of OSI architecture?
9. Note down the steps involved in communication of data in adjacent layer on the same computer?
10. How layers are interacting in different computer?

4.7 SUGGESTED READINGS

1. Computer Networks : Andrew Tanenbaum
2. TCP/ IP : Emmett Dulaney

❁❁❁

NOTES

Chapter 5

OSI Model - Physical Layer

5.0 OBJECTIVES

After studying this chapter you will be able to-

- ✓ State the lower layers of the OSI reference model
- ✓ Define the basic purpose of the OSI physical layer
- ✓ Describe the methods associated with OSI physical layer topic
- ✓ State the connection types used in computer networks.

5.1 INTRODUCTION

OSI model is the reference model for computer networking; it contains seven layers in all. The OSI layers are broadly categorized into upper layers and lower layers. The upper layers of the OSI model are:

- Application
- Presentation
- Session

The information technology organizations who are involved in designing and developing network operating systems and services to applications are mainly concerned with the protocols defined at OSI upper layers. For example, Microsoft and Novell who developed network services and related applications are mostly concerned with protocols defined at application, presentation and session layers of the OSI model.

The lower layers of OSl model are:

- Transport
- Network
- Data link
- Physical

The lower layers are oriented more towards the flow of data from end to end through the network. The organizations like Cisco, Intel, Nortel, 3com-who are involved in manufacturing of active networking components devices like hubs, bridges, switches, and routers- are more concerned with the lower four layers of the OSI model.

5.2 OSI PHYSICAL LAYER

Some companies like Lucent and Amps who aim engaged in -manufacturing of computer networking cables (fiber optics, UTP, STP etc) deal with specifications defined at physical layer of the OSI model.

This is the first layer of QSI model. This layer is concerned with transmitting raw bits over a communication channel. The design Issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit. Physical Layer defines:

- Connection types Physical topologies
- Mechanical and electrical specifications for using the transmission medium
- Bit transmission and synchronization.

The following network connectivity hardware are normally associated with the OSI physical Layer

* Repeaters, hubs, and multiplexers, which regenerates electrical signals.
* Transmission media connectors, which regenerates electrical signals interconnect devices to the transmission media.
- Modems and codecs, which performs digital and analog conversions

The hardware devices -repeaters, hubs, and multiplexers and transmission media connectors that work at Physical Layer were already discussed at length in chapter 4.

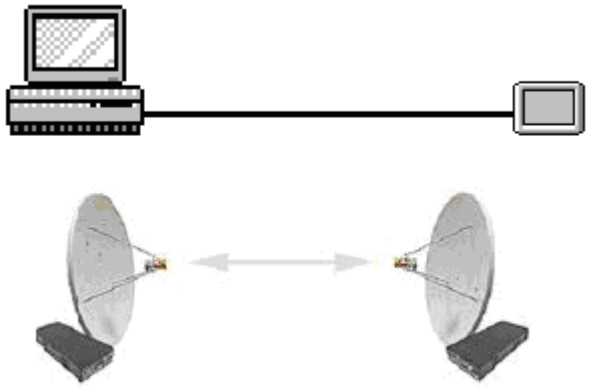
5.3 CONNECTION TYPES USED IN COMPUTER NETWORKS

Computer networks are built using point-to –point and multipoint connections. These two types of connections describe how many devices connect to a single cable or segment of transmission media.

5.3.1 Point-to Point connection

A point-to-point connection is a direct link between two devices. When you attach a personal computer directly to a printer, you have created a point-to .point link. Another example is the link between two microwave antennas. The figure given below shows point-to-point connections.

Because only two devices share a point-to point connection, each station is guaranteed a specific transmission capacity or bandwidth.

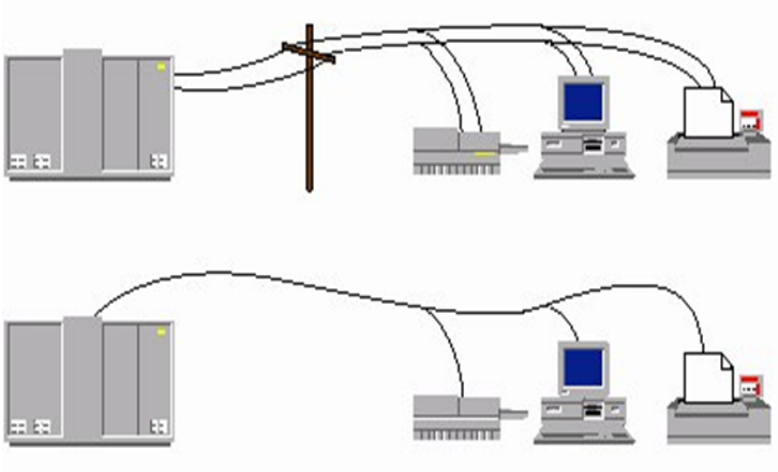


Point-to-point connections

5.3.2 Multipoint connections

A multipoint connection is a link between three or more devices. In old good days, multipoint connections were used to connect one master computer with -a series of slave-terminals. In today's LAN environment, multipoint connections link multiple devices in the bus, star, and cellular topologies described m the next subsection.

Multipoint connections share the share bandwidth so the overall capacity is divided among every device connected to the media.



Multipoint connections

Check your progress – 5.3

Answer in brief.

1. List out the lower layers of QSI module?

   ……

   ……

2. What is purpose of physical layer?

   ……

   ……

3. What are multipoint connections?

   ……

   ……

5.4 COMMON PHYSICAL TOPOLOGIES

All computer networks rely upon point-to-point and multipoint connections. However, the complete physical structure of the transmission media is called Physical topology or A topology defines the arrangement of nodes, cables, and that make up the network.

When you choose a physical network topology, pay special attention to the following characteristics: -

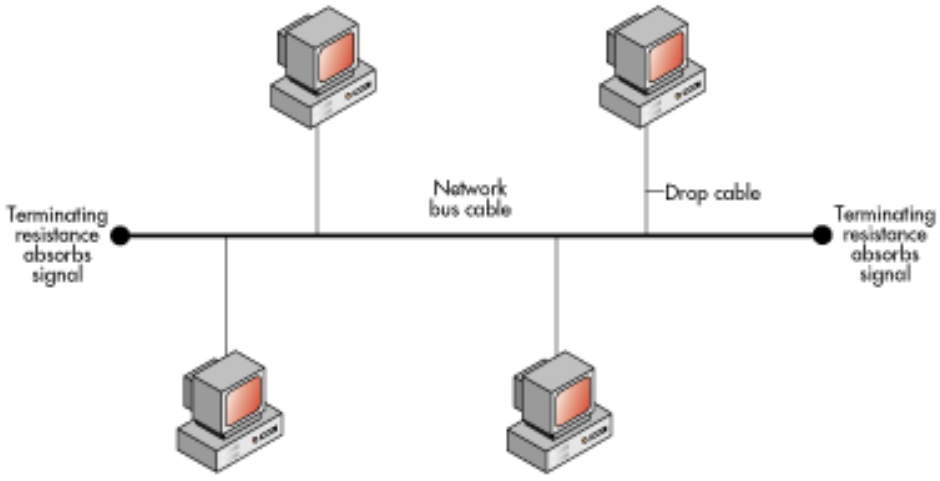
- Relative ease of installation
- Relative ease of configuration
- Relative ease of troubleshooting
- Maximum number of units affected by a media failure

Physical and logical topologies can take several forms. The most common and the most important for understanding the Ethernet and Token Ring topologies are

- Bus topology .
- Ring topology
- Start topology
- Mesh topology
- Cellular topology

5.4.1 Bus topology

A bus physical topology is one in which all devices connect to a common, shared cable. A physical bus topology network typically uses one long cable, called a backbone, Computers (workstations and servers) are attached directly to the backbone using Terrestrial microwave-connectors. The backbone is terminated at both ends to remove the signal from the wire after it has passed all devices. Most bus topologies allow electric or electro-magnetic signals to travel in both directions.



Bus Physical Topology

Advantages

1. Uses established standards
2. Relatively easy to install
3. Requires less media than other topologies

Disadvantages

1. Moderately difficult to reconfigure
2. Since a bus topology is based on a single cable, troubleshooting is relatively difficult.
3. All units affected by media failure

5.4.2 Ring topology

Ring topologies are wired in a circle. Each node is connected to its neighbors or either side, and date, passes around the ring in one direction only. Each device incorporates a receiver and a transmitter and servers as a repeater that passes the Signal to the next device in the ring. Because the signal is regenerated at each device, signal degeneration is low.

Ring topologies are ideally suited for token passing access methods. The token gets passed around the ring, and only the node that holds the token can transmit data. Ring physical topologies are quite rare.

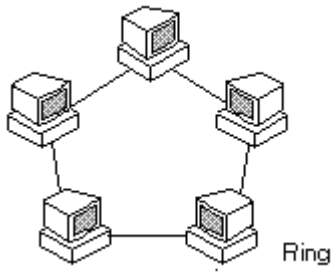
Advantages

- Because each device incorporates a repeater, you can easily find cable faults.
- Dual loop rings can be very fault tolerant.

Disadvantages

- More difficult to install and reconfigure than bus topology
- Faults in single loop system^ affect all devices on the network
- Because the ring requires a closed loop, more media is required than with bus networks.

Ring topology



5.4.3 Star Topology

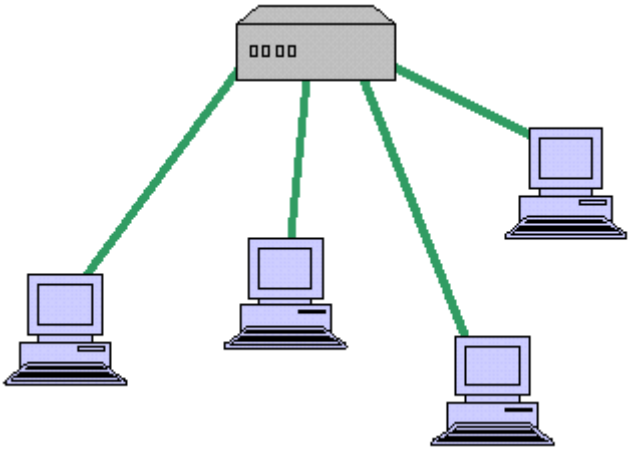
Physical star topologies use a central device with drop cables extending in all directions. Each networked device is connected via a point-to point link to the central device called a hub or multiport repeater. Additionally, star, topologies can be nested within other stars to form tree or hierarchical network topologies. In star topology, electrical or electromagnetic signals travel from the networked device, up its drop cable, to the hub, from there the signal is sent to other network.

Advantages

- Star topologies are relatively easy to reconfigure.
- Because all data in a star network goes through a central point where it can be collected, stars are easy to troubleshoot.
- Media faults are automatically isolated to the failed segment.

Disadvantages

- Star topologies require more cable than most other topologies
- Moderately difficult to install
- Hub failures can disable

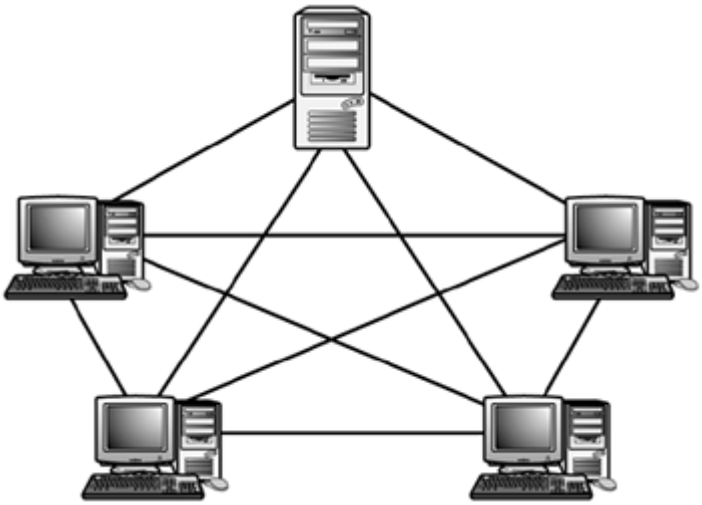


Star Topology

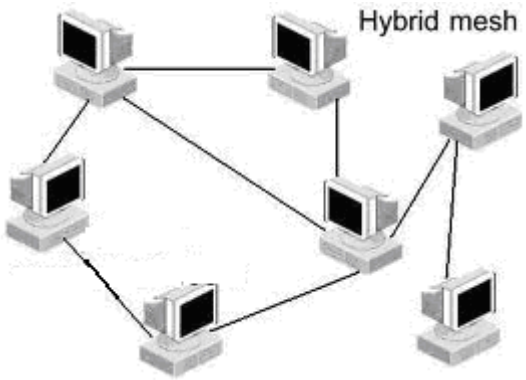
5.4.4 Mesh topology

A mesh network has point-to-point connections between every device in the network. Because each device requires an Interface for every other device on the network, mesh topologies are not usually considered practical. However, mesh networks are extremely fault tolerant, and each link provides guaranteed capacity.

Typically, you use mesh topologies in a hybrid network with just the largest or most important sites interconnected. You would use a hybrid mesh topology with redundant links between the main sites to insure continuous communications between the mainframes. The following figure will explain the topological difference between true mesh and hybrid mesh.



Mesh Topology



Hybrid Mesh

Advantages

- Mesh topologies are easy to troublesh are because each medium link is independent of all other.
- Mesh topologies resist media failure better than other topologies.

Disadvantages

- Mesh networks are relatively difficult to install because each device must be linked directly to all other devices.
- Mesh topologies are difficult to reconfigure.

5.4.5 Cellular Topology

A cellular topology combines wireless point-to-point and multipoint strategies to divide a geographic area into cells. Each cell represents the portion of the total network area in which a specific connection operates. Devices within the cell communicate with a central station or hub. Hubs are interconnected to route data across the network and to provide the complete network infrastructure.

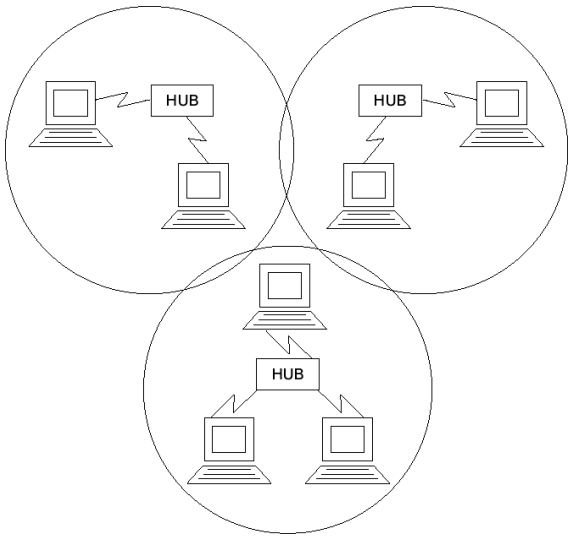
As a wireless structure, the topology that dependant upon the interconnection of cable. Cellular topology relies on the location of wireless media hubs. Because of this difference, cellular topologies exhibit qualities that are very different from cable topologies. For example, devices may roam from cell to cell while maintaining connection to the network.

Advantages

- Relatively easy to install
- Does not require media reconfiguration when adding or moving users.
- Fault isolation and troubleshooting is fairly simple.

Disadvantages

- All devices using a particular hub are affected by a hub failure.



Cellular Topology

Check your progress – 5.4

Answer in brief.

1. What is topology?

   ……

   ……

2. Explain cellular topology?

   ……

   ……

3. What are the advantages of star topology?

   ……

   ……

5.5 DIGITAL AND ANALOG SINGNALING

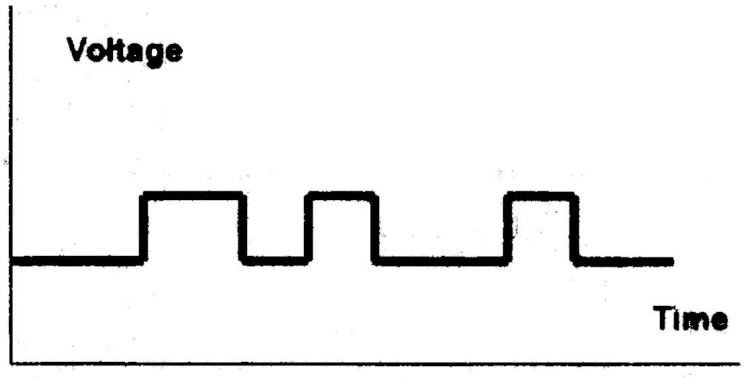
The methods for using electrical energy to communicate are called signaling there are two forms of signaling:

- Digital signaling
- Analog signaling

Both types of signals represent data through the manipulation of electric or electromagnetic characteristics. How these characteristics of status change, determines whether a signal is digital of analog.

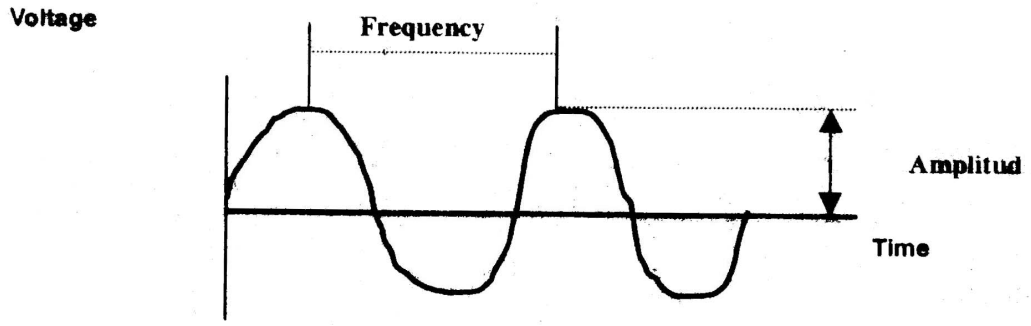
5.5.1 Digital signaling

Digital signals are represented by discrete states. It indicates time in absolute numbers such as hours and minutes. In computer networks, digital signaling is accomplished by pulses of light or electric voltages. The state of the pulse (on or off, high, or low) is changed to represent binary bits of data. The following figure is a typical representation of a digital signal.



5.5.2 Analog signaling

Analog signals rely on the continuously variable states of waves. Electromagnetic waves, used in analog signals, are often represented by the sine wave shown in the following figure.



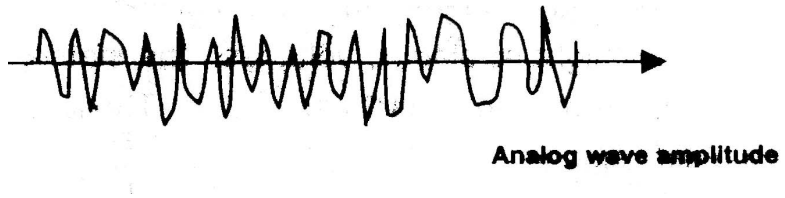
Waves are measured using one or moore of the following three characteristics:

- Amplitude
- Frequency
- *Phase*

Amplitude

You can consider the amplitude of a wave as the signal strength compard to some reference value (measured in volts). Analog signals are based upon amplitude / strength shifts, which vary constantly from positive to negative value. Amplitude is commonly expressed in

- Volts when measuring electrical potential
- Amps when measuring electrical current
- Watts when measuring electrical power
- Decibels when measuring the ratio, between the power of two signals



Frequency

The frequency of a wave is the time it takes for a wave to compete one cycle. In other words, if a signal takes one second to make a transition from high amplitude to low and back to high, the frequency of fie wave is one second. Frequency is typically measured in hertz (Hz), or cycles per second.

Phase

The phased a signal refers to the relative state of the wave when timing began,

Bit Synchronization

Data bits ate encoded on this analog or digital signal by changing the state of specific Signal characteristic. Th6 receiver interprets the signals by taking a measurement of the characteristic. Therefore the receiver must know the correct time to measure and decode the signal and extract the correct data bits.

The control of measurement timing clocks can be called bit synchronization. There are two type of bit synchronization.

1. Asynchronous
2. Synchronous

All data transmissions require some type of synchronization.

5.6 BANDWIDTH

A channel is simply a part of the media's total bandwidth. A channel is created by splitting up the multiple EM frequencies that a medium can accommodate or by dividing the entire bandwidth into units. For example, if a medium can support 10 Mbps, two channels can be created at 5 Mbps each. If a medium can support EM waves with frequencies between 1 MHz and 10 GHz, multiple channels could be created using 1 MHz, 10MHz, 100MHz, 1GHz, and 10GHz signal

The following names have been given to bandwidth use schemes:

1. Baseband
2. Broadband

The transmission capacity your networks transmission media can provide is dependant upon the bandwidth used by method you use.

1. Baseband

Baseband systems use the transmission medium's entire capacity for a single channel. Baseband networks can use either analog or digital signaling, but digital is much more common. A baseband connection sends signals without modulation over twisted-pair, coaxial, or fiber optic cable. Multiple signals can be sent over the same baseband connection by using a technology called TDM. Usually baseband signals can be more reliably interpreted and regenerated than broadband signals.

2. Broadband.

Broadband systems used the transmission media’s capacity to proves, multiple channels. Multiple channels are created by dividing the medium's bandwidth by using a technology FDM. Each channel is protected from the others by guard channels. small bands of unused frequency placed in between the data channels. Using analog signals, broadband networks can directly support multiple simultaneous conversations.

5.7 SUMMARY

- ✓ In this chapter we studied OSI model is the reference model for computer networking. It contains seven layers in all
- ✓ OSI Physical Layer is the first layer of OSI model. This layer is concerned with transmitting raw bits over a communication channel.
- ✓ A topology defines the arrangement of nodes, cables, and connectivity devices that make up the network. Physical and logical topologies can take several forms.
    - Bus topology
    - Ring topology
    - Star topology
    - Mesh topology
    - Cellular topology

5.8 CHECK YOUR PROGRESS – ANSWERS

1. The lower layers of OSI model are:

- Transport
- Network
- Data link
- Physical

2. The OSI-Physical layer is concerned with transmitting raw bits over a communication channel.

3. A multipoint connection is a link between three or more devices. Multipoint connections link multiple devices in the bus, star, and cellular topologies.

5.4.1 to 5.4.4

1. A topology defines the arrangement of nodes, cables, and connectivity devices the make up the network.

2. A cellular topology combines wireless point-to-point and multipoint strategies to divide a geographic area into the cells. Each cell represents the portion of the total connection operates. Devices within the cell or hub. Hubs are interconnected to route vide the complete network infrastructure.

3. Advantage of Star Topology

* Star topologies are relatively easy to reconfigure.

* Because all data in a star network goes through a central point where it can be collected, stars are easy to troubleshoot.

5.9 QUESTIONS FOR SELF – STUDY

1. Write note on

1. Connection types used in computer networks
2. Bus topology
3. Cellular topology
4. Advantages and disadvantages of ring topology
5. Purpose of OSI physical layer

2 Choose correct answers.

a. Which physical topology a central device with drop cables extended in all directions? a) Bus Ring b) Star c) Mesh

b. What types of connection enable multiple devices to be on the same media simultaneously?

a) Transport b) point-to-point multipoint c) all of above

c. Which -of the following can be the physical topology of a network?

a) Point-to-point baseband & broadband b) Ring, star, ring, bus, mesh, cellular

3. Which of the hardware devices operates at OSI layer 1?

4. Explain Analog signaling?

5. Write a note on bandwidth used in physical layer?

5.10 SUGGESTED READINGS

1. Computer Networks : Andrew Tanenbaum
2. Cisco CCNA Certification Guide : Wendell Odom

❁❁❁

NOTES

Chapter 6

OSI-Data Link Layer

6.0 OBJECTIVES

After studying this chapter you will be able to-

- ✓ Explain basic purpose of OSI-Data Link Layer
- ✓ Describe the networking technology topics associated with OSI Data Link Layer
- ✓ Identify and describe the methods associated with OSI Data Link Layer topic.

6.1 INTRODUCTION

The second layer is the Data Link layer. It is responsible for the creation and interpretation of different frame types based on the actual physical network being used. For instance, Ethernet and Token-ring networks support different and numerous frame types, and the Data link layer must understand the difference between them. The layer is also responsible for interpreting what it receives from the physical layer, using low level error detection and correction algorithms to determine when information need to be re-sent.

6.2 FUNCTIONS OF DATA LINK LAYER

The following are the basic functions of data-Link Layer:

- Arbitration- Determines when it is appropriate to use physical medium.
- Addressing- ensures that the correct recipient(s) receives and processes the data that is sent.
- Error detection- Determines Whether the data made the trip across the medium successfully.
- Identifying the encapsulated data (frame identification)- Determines the type of header that follows the data link header.

Like most other layers, the Data Link Layer adds its own control information to the front of the data packet (header) and at the end of the data packet (trailer). This information may include a source and destination address (hardware or MAC address), frame length, indication of protocols used by higher layer, frame check sequence (FCS) etc.

The following network connectivity devices are normally associated with the OSI Data Link layer:

- Bridges

- Switches
- Intelligent Hubs
- Network interface boards.

The four functions (mentioned above) of Data Link layer are normally split between the following two sub layers.

1. Media Access Control (MAC)
2. Logical Link Control (LLC)

6.3 MEDIA ACCESS CONTROL

MAC sub layer controls the way transmitters share a signal transmission channel it includes following topics.

1. Logical topology
2. Media access
3. Addressing

6.3.1 Logical topology

Network entities transmit data depending upon the network's logical topology. Physical topology discussed earlier is the structure of media or data path. In some special cases, a physical network topology will not reflect the way the network Operates. The actual signal path is called a logical topology.

A good example of disparate physical and logical topologies is an IBM Token-Ring Network. Token-Ring LANs often use copper 'cable arranged in a star topology with a hub at center. The hub does not repeat incoming signals to all other attached devices, as in normal star topology.

The hub's circuitry distributes incoming signal to the next device in a predetermined logical ring. Therefore the physical topology employed is a star, while the logical topology is a ring. To determine the logical topology of the network, you must understand how signals are received on your network:

- In logical bus topologies, every signal received by all devices.
- In logical ring topologies, each device only receives signals that have been specifically sent to it.

6.1 to 6.3.1 Check your progress

Answer in brief.

1. What is the purpose of Data Link Layer?

   ……

   ……

2. Explain the functions of Data Link Layer?

   ……

   ……

3. List the network connectivity device, which are normally associated with the Data Link Layer?

   ……

   ……

4. Define – Logical Topology ?

   ……

   ……

6.3.2 Media Access

Logical topologies use specific rules that control when network entities are allowed to transmit data signals. The control process is called media access. If access rules are not observed, and devices transmit whenever they are, ready, sometimes they may transmit at the same time, and that creates a collision. The collision destroys effective communications. You cannot operate a network unless you can control or eliminate, the effects of collisions. The mechanism of controlling collision is called arbitration. The following media access methods describe rules that govern when network devices are allowed to transmit:

- Contention
- Token-passing
- Polling

1) Contention

Contention systems are based on the philosophy that media access should be allowed on a first-come, First-served (FIFO) basis. In other words, each network device contends for control of the media.

Ethernet uses the carrier sense multiple access collision detect (CSMA/CD) Protocols or algorithm for arbitration. The basic algorithm for using an Ethernet when there is data to be sent consists of the following steps:

Step1 Listen to find out whether a frame is currently being received.
Step 2 If no other frame is on Ethernet, send.
Step 3 If another frame is on Ethernet, wait and then listen again.
Step 4 While sending, if a collision occurs, stop, wait, and again listen.

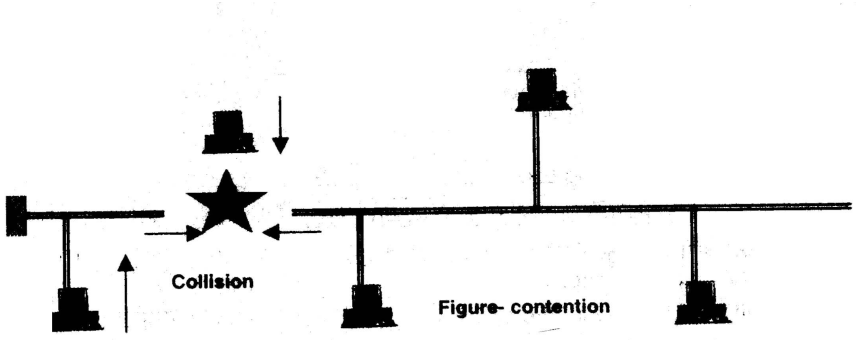


Figure- contention

CSMA/CD protocols are quite popular. DEC's Ethernet version 2, Local Talk, and IEEE 802.3 are examples of CSMA/CD protocols.

Advantages

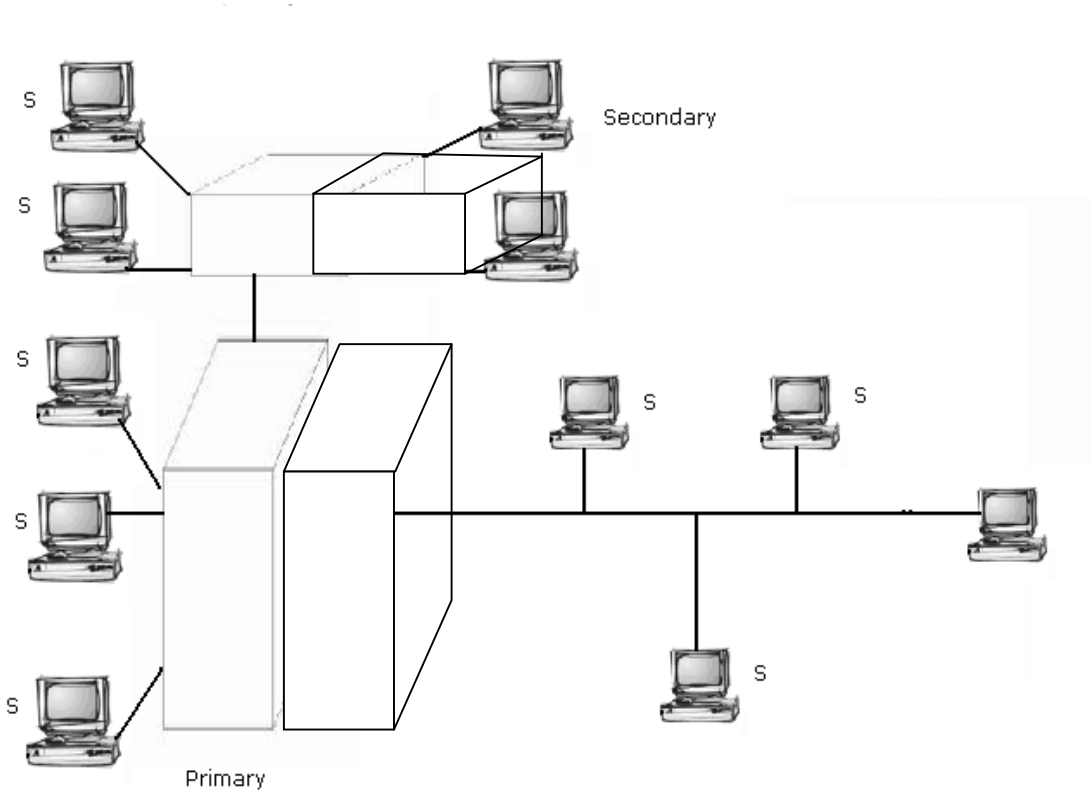
- Software is relatively very simple and produces very little overhead.
- Immediate and complete control over media, as long as no other network device has access.
- At low traffic levels, actual data through put is usually very high.

Disadvantages

- Access times are not predictable (called probabilistic).
- Priorities cannot be used to give faster access to some devices.
- Collisions increase geometrically with the addition of new devices.

2) Token-passing

With Token Ring, a totally different mechanism is used. A free-token frame rotates around the ring while no devices has data to send. When sending, a device claims the free token, which really means changing bits in the 802.3 headers to signify "token busy" state. The data is then placed onto the ring after the Token Ring header.



Token Passing

The basic algorithm (or protocols) for using a Token Ring when there is a data to be sent consists of the following steps:

Step1 Listen for the passing token

Step 2 If token is busy, listen for the next token.

Step 3 If the token is free, mark the token as a busy token, append the data, and send the data onto the ring.

Step 4 When the header with the busy token returns to the sender of that frame, after Completing a full revolution around the ring, the sender removes the data from the ring.

Step 5 The device sends a free token to allow another station to send a frame.

Several token-passing protocols are available. Two token-passing LAN standards are the IEEE 802.4 Token Bus and 802.5 Token-ring. The Token Bus network uses token-passing access control and a physical or logical bus topology, while the Token Ring network uses token-passing access control arid a physical or logical ring topology. Another token-passing standard (for fiber-optic LANs) is called FDD I, which stands for fiber-distributed data interface.

Token-passing networks are appropriates for networks with time sensitive traffic of set priority, such as digital voice or video, or heavily populated networks.

Advantages

- Token passing produces predictable load and delay (therefore, it is called deterministic).
- Priorities can be assigned to ensure faster access for some secondaries.
- Eliminates collisions and may offer the highest network data throughput possible under high-load conditions.

Disadvantages

- Requires relatively complicated interactive software in all devices, which need to be reasonably intelligent.

- Device software parameters need to be adjusted each time a device is added to or taken off the media.
- Some Token Rings require an additional central controller for fault detections and recovery.

3) Polling

Polling is an access method that designates one device (called a controller, primary or master) as a media access administrator. These device requires each of the other devices (refereed as secondaries) in some predetermined order to see whether they have information to transmit. To get data from secondaries, the primary sends a request for data to the secondary, and then receive data the secondary sends. The primary then polls another secondary and receives the data that secondary can transmit after a poll. Polling systems are ideal for networking time-sensitive devices, such as automation equipment.

Advantages

a. Centralises channel access for greater network control

b. Maximum and minimum access times and rates on the channel are predictable and fixed (called deterministic).

c. Priorities can be assigned to assure faster access.

d. Allows complete use of the media's capacity eliminating collisions.

Disadvantages

a. Delays, while other devices are being polled; may be unacceptable for some application.

b. Uses a lot of bandwidth sending notices and acknowledgements or listening for messages.

c. Involves more overheads than the other media access methods.

IEEE standards of protocol

The IEEE (institute of Electrical and Electronic engineers) is the largest professional organization in the world. The 802 subcommittee of that organization has developed a series of standards govern lower layer protocols and interactions with transmission media. Recognized and reissued by the ISO, they are also known as the ISO 802 standards.

802.X standards series

IEEE802.1	802.1 standards defines internetworking
IEEE 802.2	Defines an LLC sub layer that is used by other lower-layer protocols. Because these lower layer protocols can use a single LLC protocol layer, Network layer protocols can be designed independently of both the network's physical layer and MAC sub layer implementation.
IEEE 802.3	Defines a network derived from the Ethernet network originally developed by Digital, Intel, and Xerox, this standard defines characteristics related to the MAC sub layer of the data link layer and the OSI physical layer.
IEEE 802.4	Describes a network with a bus physical topology that controls media access with a token mechanism. This standards was designed to meet the needs of industrial automation system but has gained little popularity. Both baseband and broadband configurations are available.

IEEE802.5	802.5 standards was derived from IBM's token ring network, which employs a ring logical topology and token-based media access control. Data rates of 14 and 16 Mbps have been defined for this standards
IEEE 802.6	The standard describes a MAN standard called Distributed Queue Dual Bus. Much more than a data network technology. This suited to data, voice, and video transmission.
IEEE 802.7	Represents the Broadband Technical Advisory group
IEEE 802.8	Represents the Fibre-Optic Technical Advisory group
IEEE 802.9	Integrated voice/ Data Networks
IEEE 802.10	Standards defines network security
IEEE 802.11	Is a standard for wireless LANs
IEEE 802.12	Demand priority Access LAN, 100 BaseVG any LAN

6.3.3 Addressing

Computer network entities need some way 49 distinguish devices on the network. This is done through addressing. The Data Link Layer is only concerned with physical devices addresses. Physical device addressee are, unique hardware addresses typically assigned by hardware venders. The hardware vendors use addresses that are allocated to them by a standards organization, the format of the address depends upon the media access method being used.

With Ethernet and Token Ring, the addresses are very similar. Each uses Media Access Control (MAC) addresses

Check your progress - 6.3

Answer in brief.

1. What are the disadvantages of contention?

……

……

2. Explain the term “arbitration?

……

……

3. Which method of media access provides a centralize administration?

……

……

4. What are the standards for IEEE 802.4 protocol?

……

……

6.4 LOGICAL LINK CONTROL

The Logical Link Control (LLC) sub layer of Data Link Layer establishes and maintains the link for transmitting data frames from one device to the next. It includes the following topics.

- Transmission synchronization
- Connection services

The following three strategies are common form of flow control:

- Static window flow control
- Dynamic wind
- Guaranteed rate flow control

Static window flow control

Static window flow control protocols can use one window size. At a given point of time it can handle definite number of frames depending upon the window size. If the sending application has sent out all frames, it must wait until one of the assigned numbers is acknowledge before it can send out another frame.

Dynamic window flow control

At times, it would be more efficient to allow network devices to adjust the window: size, this is referred to as dynamic, floating, or sliding window flow control. The number of permissible outstanding frames varies according to current status of the receiver. When the receiver's buffer exceeds a specific level, it sends out a choke packet. This notify sender to slow down. After complying with the choke packet, the sending application slowly increases the transmission rate until another choke packet is sent. In this way, the window size is constantly adjusted up or down.

Guaranteed rate flow control

Guaranteed rate flow control is set up before data transmissions are sent. The sending and receiving applications agree upon an acceptable transmission rate for the entire conversation, and this rate is guaranteed for as long as the conversions lasts.

Error Detection

LLC-level error detection simply refers to the process of learning whether bit errors occurred during the transmission of the frame. To do this, most data link includes a frame check sequence (PCS) or cyclical redundancy check (CRC) field in the data link trailer. This field contains a value that is the result of mathematical formula applied to the data in the frame. The PCS Value calculated and sent by the sender should match the value calculated by the receiver.

Error detection does not imply recovery. Most data links, including 802.5 Token Ring and 802.2 Ethernet, do not provide error recovery. In these two cases, however an option in the 802.2 protocols LLC type 2 does perform error recovery.

Check your progress - 6.4 & 6.5

Answer in brief.

1. What is isochronous transmission?

   ……

   ……

2. What is a difference between synchronous and asynchronous transmission?

   ……

   ……

3. Explain the functions of connection services?

   ……

   ……

4. What is flow control?

   ……

   ……

6.5 SUMMARY

- ✓ The second OSI layer is the Data Link layer. It is responsible for the creation and interpretation of different frame types based on the actual physical network being used. The layer is also responsible for interpreting what it receives from the physical layer, using low level error detection and correction algorithms to determine when information need to be re-sent.

- ✓ The layer is also responsible for interpreting what it receives from the physical layer, using low level error detection and correction algorithms to determine when information need to be re-sent.

- ✓ Data Link layer are normally split between the following two sub layers. Media Access Control (MAC) and Logical Link Control (LLC)

6.6 CHECK YOUR PROGRESS – ANSWERS

6.1 to 6.3.1

1. OSI-Data Link Layer is mainly responsible for the creation and interpretation of different frame types based on the actual physical network being used. In addition to this, the layer is also responsible for interpreting what it receives from the physical layer, using low level error ejection and correction algorithms to determine when information need to be re-sent.
2. The following are the basic functions of Data Link Layer:

- Arbitration- determines when it is appropriate to use physical medium.
- Addressing- ensures that the correct recipient(s) receives and processes the data that is sent.
- Error detection- determines whether the data made the trip across the medium successfully. Identifying the encapsulated data (frame identification)- Determines the type of header that follows the data link header.

3. The following network connectivity devices are normally associated with the OSI Data Link layer:
    - Bridges
    - Switches
    - Intelligent Hubs
    - Network interface boards.
4. Logical topology- the actual signal path is called a logical topology.

6.3.2 to 6.3.3

1. Disadvantages of contention-

- Access times are not predictable (called Probabilistic).
- Priorities cannot be used to give faster access to some devices.
- Collisions increase geometrically with the addition of new devices

2. Sometimes devices transmit at same time, and that creates collision, which destroys effective communication. The mechanism of controlling collision is called as arbitration.
3. 'Polling' method of media access provides a centralise administration.
4. Standards for IEEE 802.4 protocol-
    - It describes a network with a bus physical topology that controls media access with a token mechanism

- Both baseband and broadband configurations are available

6.4 & 6.5

1. Isochronous transmissions methods use a constant fixed-frequency transmission clock to create set time slots. A clock signal is generated by a designated network device and is passed to all other devices on the network.
2. Difference between synchronous and Asynchronous transmission-
   - Asynchronous transmission methods rely upon the transmitting and receiving devices to maintain their own internal clock.
   - In asynchronous transmission, the two devices use similar timing but do not synchronize their clocks.
   - Synchronous transmission methods require that the communicating devices take responsibility for providing a transmission (or framing) clock.
   - These transmissions resist timing errors much better than asynchronous, because both the transmitter and receiver use same clock.
3. Connection services perform the following functions
   - Control the amount of data transferred from one computer to the next
   - Detect transmission errors and request retransmissions
4. Flow control is a set of rules to regulate how much data can be transmitted within a specified time.

6.7 QUESTIONS FOR SELF – STUDY

1. How are physical and logical topologies different?
2. Which sub layer controls the Way transmitters share a signal transmission channel?
3. Which media access method operates on a first come, first served baste?
4. What is contention? Explain
5. Explain the advantages and disadvantages of Token-ring passing?
6. Explain the different types of flow control methods?
7. What are the functions of Data Link Layer?
8. List the networking devices operate at OSI layer 2?
9. What is logical topology?
10. Explain the term error detection?

6.8 SUGGESTED READINGS

1. Computer Networks : Andrew Tanenbaum
2. Computer Networks : Tanenbum

❁❁❁

NOTES

Chapter 7

OSI Reference Model- Network and Transport Layer

7.0 OBJECTIVES

After studying this chapter you will be able to-

- ✓ Distinguish between OSI Data Link and Network layers addressing
- ✓ Identify and describe the OSI networking layer function
- ✓ Identify the Layer 3 address structures and associated protocols
- ✓ Explain the concepts of route selection and route discovery
- ✓ Compare and contrast connectionless and connection oriented protocols
- ✓ Describe the OSI Transport Layer function
- ✓ Identify and describe three methods of flow control at Transport layer.

7.1 INTRODUCTION

In this chapter we are learning third and fourth layer of OSI model

The Network layer is concerned with getting packets from the source all the way to the destination. Getting to the destination may require making many hops at intermediate routes along the way. This function clearly contrasts with that of the data link layer, which has the move goal of just moving frames from one end of wise to the other. Thus network layer is the lowest layer that deals with end – to – end transmission.

The difference between DLL and Network layer are explained. The primary objective of the network layer is to move data to specific network locating. This appears similar to what the data link layer accomplishes through physical device addressing. Data link layer addressing operates on a single network. The network layer describes method for moving informal between multiple independent networks, called internetworks.

Data link layer addressing delivers data to all devices attached to single network and relies upon the receiving devices to determine whether the data was meant for it.

This layer choose a specific route through an internetwork and avoid sending data to uninvolved network. This layer does this through switching, addressing and routing layer algorithms. This layer is also responsible for ensuring correct data routers through an internetwork of dissimilar networks.

The network layer is concerned with getting packets from the source all the way the destination may require making many hops at way. This function clearly contrasts with that of the data modest goal of just moving frames from one end of wire to yhe other. Thus the network layer is the lowest layer that deals with end-to-end transmission.

To achieve its goal the network layer must know about the topology of the communication subnet (i.e the set of all routers) and choose appropriate paths through it. It must also take care to choose routes to avoid overloading some of the communication lines and routers while leaving others idle. Finally when the source and destination are in different networks, it is up to the network layer to deal with this differences and solve the problems that results from them.

7.2 DIFFERENCE BETWEEN DATA LINK AND NETWORK

As discussed above, the primary objective of the network layer is to move data to specific network locations. This appears similar to what the Data Link layer accomplishes through physical device addressing. However, data link layer addressing operates on a single network. The network layer describes methods for moving information between multiple independent networks, called internetworks.

Data link layer addressing delivers data to all devices attached to a single network relies upon the receiving devices to determine whether the data was meant for it. In contrast, the network layer choose a specific route through an internetwork and avoid sending data to uninvolved networks. The network layer does this through switching, network layer addressing, and routing layer algorithms. The network layer is also responsible for ensuring correct data routes through an internetwork of dissimilar networks.

7.3 OSI NETWORK LAYER FUNCTIONS

Following are the three major functions performed at Network Layer

- Routing
- Addressing
- Switching

7.3.1 Routing

Routing can be thought of as a three-step process as shown in the figure given below :

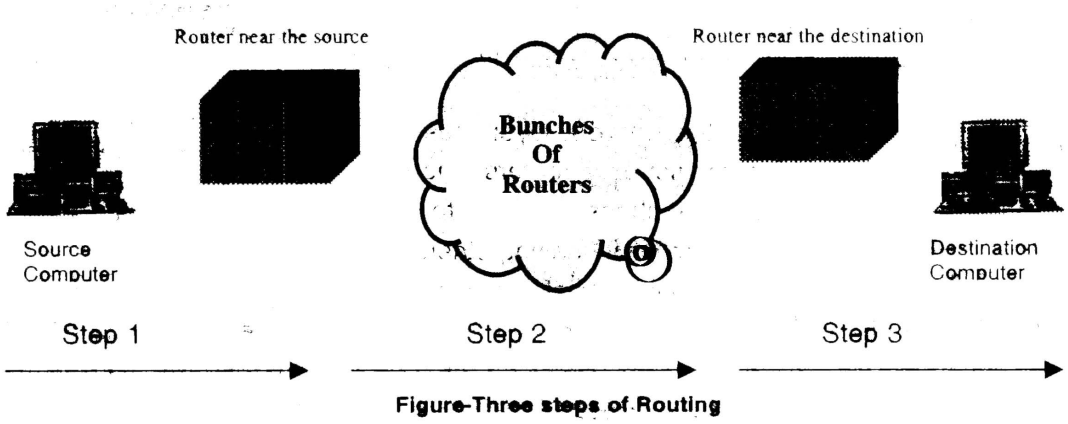


Figure-Three steps of Routing

Step 1 - Sending the data from the source computer to some nearby router.

Step 2- Delivering the data from the, router pear the source to a router near the destination.

Step 3- Delivering the data from the router near the destination to the end destination computer.

1) Sending data to a nearby router

The creator of the data, who is also the sender of the data, decides to send data to a device in another group. A mechanism must be in place so that the sender knows of some router on a common data link with the sender to ensure that data can be send to that router.

The sender sends the data link frame across the medium to the nearby router (Layer 2) addressing in the data link header to ensure that the nearby router receives the frame.

2) Routing Data Across the Network

To route the data packet across the network. A router uses the routing table for a particular network layer protocol type which is nothing more than a list of network layer address groupings. These groupings vary based on the network layer protocol type. The router compares the destination network layer address in the packet to the entries in the routing table in memory, and a match is made. This matching entry in the routing table tells this router where to forward the packet next.

Any intervening routers repeat the same process. The destination network layer (Layer 3) address in the packet identifies the group in which the destination resides. The routing table is searched for a matching entry, which tells this router where to forward the next packet. Eventually, the packet is delivered to the router connected to the network or subnet of the destination host.

3) Delivering data to the end destination

When the packet arrives at a router sharing a data link with the true destination, the route and the destination of the packet (end device) are in the same L3 grouping.

The final router can forward the data directly to the destination (end device). As usual, a new data link header & trailer are created before a frame (which contains the packet that made the trip across the entire network) can be sent on to the media. This matches the final step (step 3), as shown in the figure.

The two important concepts in routing are Route selection and Route discovery, which have been briefly explained in following paragraph.

Route selection

Route selection is the ability to determine which route will be the most efficient to use to forward data to its final destination. Cost is the number assigned to a link, or route, to give it a relative priority. In the area of cost, the link with the least assigned cost is the first to be selected. One-way of determining cost is the number of hops, which is the number of routers that data packet must pass through to reach the destination network. A factor in cost determination can also be time, sometimes calculated in the form of ticks, which are a time period of 1/18 of a second.

Route discovery

Route discovery is performed by a routing protocol, of which there are two types:

Distance vector and link-state. Each type of routing protocol handles route discovery in a, different way. Routing information protocols (RTP – 1, TRP – 2) and interior Gateway Routing Protocol (1GRP) are the examples of distance vector protocols, while Open Shortest Path first (OSPF) is an example of link state protocol.

7.1 to 7.3.1 Check your Progress.

A) Answer in brief

1. What is the purpose of Network layer?

   ……

   ……

2. What is the difference between data link layer and network layer transmission?

   ……

   ……

3. Explain the second step in routing?

   ……

   ……

4. What is route selection?

   ……

   ……

B) Fill in the Blanks

1) ……., ……. and ……. are three major functions of network layer

2) ……. Is ability to determine which route is more efficient to forward data to its final destination.

3) Route discovery is performed by a ……..

7.3.2 Addressing

One key feature of network layer addresses in that they were designed to allow logical grouping of addresses. In TCP/IP, this group is called a network or a subnet. In IPX. It is called a network. In AppleTalk, the grouping is called a cable range.

Network layer addresses are also grouped based on physical location in a network. The rules differ for some network layer protocols, but the grouping concept is identical for IP, IPX, and AppleTalk. In each of these network layer protocols, all devices with addresses in the same group cannot be separated from each other by a router that is configured to route that protocol, respectively.

A is best exemplified in TCP/IP The most fundamental element of the Internet protocol is the address space that IP uses. Each machine on a network is given a unique 32-bit address called as Internet address or IP address. Addresses are divided into five categories, called classes. There are currently A, B, C, D and E classes of addresses.

The unique addresses given to a machine if derived from the class A, B, or C addresses. Class D addresses are used for combining machines into one functional group, and class E addresses are considered experimental and are not currently available. For now, the most important concept to understand is that each machine requires a unique address and that IP is responsible for maintaining, utilizing, and manipulating it to provide communication between two machines. The whole concept behind uniquely identifying machines is to be able to send data to one machine and one machine only, even in the event that the IP stack has to broadcast at the physical layer, the form of packets from the Transport layer, from either TCP or UDP, and

sends out data in what are commonly referred to as datagrams. The size of a datagram depends on the type of network that is being used, such as token ring or Ethernet. If a packet has too much data to be transmitted in one datagram, it is broken into pieces and transmitted through several datagrams. Each of these datagrams then has to be reassembled by TCP or UDP.

Most network layer (layer 3) addressing schemes were created with following goals :

- The address space should be large enough to accommodate the largest network with a selected layer-3 addressing protocol.
- The address should allow for unique assignment so that little or no chance of address supplication exists.
- The address structure should have some grouping implied so that many addresses are considered to be in the same group.
- In some cases, dynamic addresses assignment is desired.

Each layer-3 address structure contains at least two parts. One or (more) part at beginning of the address, which identifies the grouping. The other or (last) part of the address acts as a logical group.

7.3.3 Switching

Switching is the method of moving data through a network where multiple redundant paths exist between the source and destination. The three major types of switching are :

1. Circuit Switching
2. Message Switching
3. Packet Switching

• Circuit Switching -

Circuit Switching establishes a path that remains fixed for/the duration of the connection. It's similar to telephone switching equipment. In the telephone world, switching equipment establishes a route between your telephone In the Midwest and a telephone in New York and maintains that .connection for duration of your call. The next time you call, the same path may or may not be used.

The advantages of circuit switching include the use of dedicated paths and a well-defined bandwidth. The disadvantages include the establishment of each connection (which can be time-consuming) and the inability of other traffic to share the dedicated media path. The latter can lead to inefficiently utilized bandwidth. Due to the need to have excess (or rather a surplus of) bandwidth, this technology tends to be expensive when compared to other options.

• Message Switching

Message switching treats each message as an independent entity and not concerned with what came before or will come after. Each message carries its own address information and details of its destination. The information is used at each switch to transfer the message to the next switch in the route. Message switches are programmed with information concerning other switches in the network that can be used to forward message to their destinations. They can also be programmed with information about which of the routes is most efficient, and they can send different messages through the network to the same destination via different routers.

In the message switching the complete message is sent from one switch to the

next, and the whole message is stored there before being forwarded. Because the switches hold what is come in and wait until it is all there before sending anything out, they are often called store-and-forward network. Common uses of this technology uses include e-mail, calendaring, and groupware applications.

The advantages of message switching are that it can use relatively low cost devices, data channels are shared among communicating devices, priorities can be assigned to manage traffic, and bandwidth is used rather efficiently. The disadvantage is that it is completely unacceptable for real time application.

• Packet Switching

When most administrators think of adding switches to their network, they think of packet switches. Here, messages are divided into smaller packets, each containing source and destination address information. They can be routed through the internetwork independently. Packet is restricted to the point where the entire packet can remain in the memory of the switching devices, and there is no need to temporarily store the data anywhere. For this reason, packet switching routes the data through the network much more rapidly and efficiently than is possible with message switching.

There are many types of packet switches. The most common are datagram and virtual circuit. When datagram packet switching, each switch node decides which network bypass busy segments and take other steps to speed packets through the internetwork making datagram packet switching ideally suited for LANs.

Virtual circuit packet switching establishes a formal connection between two devices and negotiates communication parameters such as the maximum message size, communication window, network path, and so on, thus creating a virtual circuit that remains in effect until the devices.

7.3.2 to 7.3.3 Cheek your progress

Define the following

a. Internet Address

……..……

……

b. Classes

……

……

c. Switching

……

……..

d. Circuit Switching

……..

……

7.4 INTROUDCTION TO OSI – TRANSPORT LAYER

The fourth layer is the Transport layer. It is primarily responsible for guaranteeing delivery of packets transmitted by the Network layer. Although it doesn't

always have to do so. The layer is desired to hide the characteristics of the computer network structure from the upper-layer process. It organizes higher-level messages into segments and reliably delivers segments to session, or higher layer processes.

The transport layer often compensates for lack of reliable, or connection oriented, connection services in the lower layers. Transport layer protocol implementations can usually confirm or deny data delivery. If data is not delivered to the receiving device correctly, the transport layer can initiate retransmission or inform the upper layers. The upper layers can then take the necessary corrective action or provide the user with options.

Connection-oriented versus connectionless protocols -

Most people correlate connection-oriented protocols with reliable or error recovering protocols because the two features are often implemented by a single protocol. However, connection oriented protocol do not have to provide error recovery, and error-recovering protocols do riot have to be connection-oriented.

Following are the definitions of connection-oriented and connectionless protocols:

Connection-oriented protocol

A protocol that either requires an exchange of messages before data transfer begins or has a required pre-established correlation between two end points.

Connectionless protocol:

A protocol that does not require an exchange of messages and that does not require a pre-established correlation between two endpoints.

The definitions are sufficiently general so that all cases can be covered. TCP is connection oriented because a set of three messages must be completed before data is exchanged. Likewise SPX is connection-oriented. Frame relay, when using PVCs, does not require any messages be sent ahead of time, but it does required predefinition in the frame relay switches, establishing a connection between two Frame Belay attached device. For the similar reasons, ATM PVGs are also connection – oriented. Connection oriented protocols are often Relay and ATM ate two examples protocol does not provide of connection-oriented error recovery or not.

Protocol characteristics: recovery and connection

Connected	Reliable	Examples
Connection-oriented	Yes	LLC type 2(802.2), (TCP/IP),SPX(Netware)
Connection-oriented	No	Frame Relay virtual circuits,
Connectionless	Yes	Frame Relay virtual circuits, ATM virtual connection, PPP
Connectionless	No	UDP, IP, IPX, Apple Talk DDP, Most layer 3 protocols

The most typical option is for a protocol to be connectionless and not perform error recovery, or to be connection oriented and to also perform error recovery. Networking professionals should be able to distinguish between error detection and error recovery. Any header pr toiler with a frame check sequence (PCS) or similar field can be used to detect bit errors in the PDU. Error detection uses the FCS to detect the error, which results in discarding the PDU. However, error recovery implies that the protocol reacts to the lost data and some now causes the data to be retransmitted.

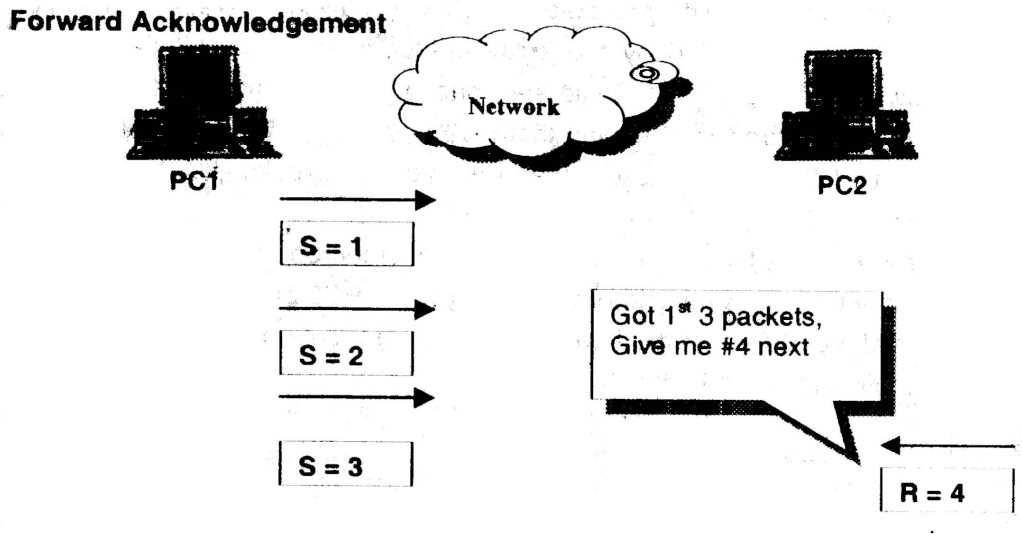
7.5 OSI TRANSPORT LAYER FUNCTIONS

Two important functions performed by recovery and flow control. The following subsections cover these two functions in detail

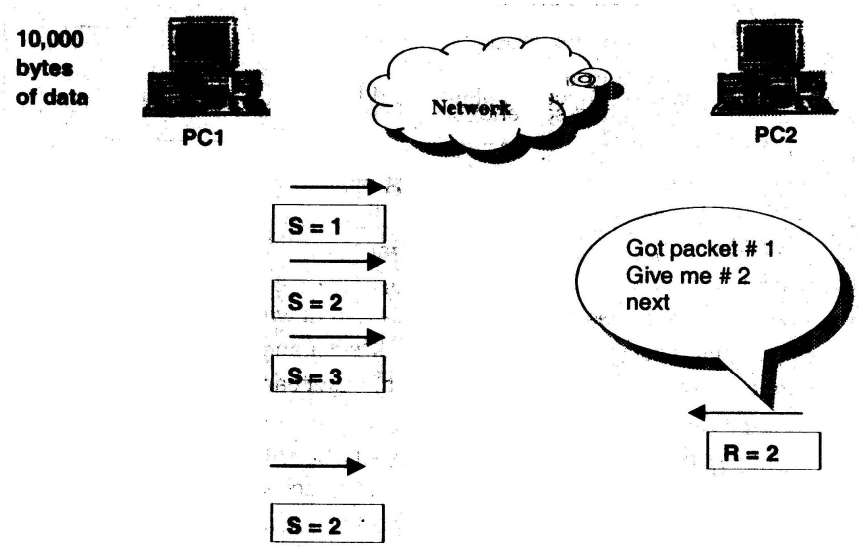
7.5.1 Error Recovery

Regardless of which protocol specification performs the error recovery; all work in basically the same way. Normally, the transmitted data is labeled or numbered. After receipt, the receiver signals back to the sender that the data was received, using the same label or number to operation.

Forward Acknowledgement



As mentioned in the above figure, the data is numbered, as shown with the numbers 1,2, and 3 these numbers are placed into header used by that particular protocol; for example, the TCP header contains similar numbering fields. When PC2 sends his next packet to PC1; PC2 acknowledges that all three packets were received by setting his acknowledgment field to 4. The number 4 refers to the next data to be received, which is called forward acknowledgement. That means that the acknowledgement number in the header identifies the next data that is to be received, not the last one received. In the following figure, the concept of error recovery is explained.



In the above figure, PC1 sent three packets numbered 1,2,and 3. But it seems that there is some error in transmitting packet #2, so PC2 is asking for retransmitting of packet #2 again. This is indicated by the acknowledgment packet (R=2) sent by PC2.PC1- got now, two choices. PC1 could sent packet numbered 2 and 3 again, or PC1 could send packet #2 and wait, hoping that pC2's next acknowledgment will say R=4 indicating that PG2 just got packet #2 and already had packet from earlier transmission.

Finally error recovery typically uses two sets of counter one to counter data in one direction, one to count data in opposite direction. So when PC2 acknowledged field in the header, the header would also have a number sent field that identifies the date in the PG2 packet.

Check your Progress - 7.4 & 7.5.1

1. What is purpose of Transport Layer?

   ……

   ……

2. Define – connection – oriented protocol connectionless protocol.

   ……

   ……

3. Explain the two important functions of transport layer?

   ……

   ……

7.5.2 Flow control

Row control is the process of controlling the rate at which a computer sends a data. Depending on the particular protocol both the sender and the receiver of the data (as well as intermediate routers, bridges, or switches) might participate in tile process of controlling the flow from sender receiver.

Flow control is needed because data is discarded when congestion occurs sender of data might be sending the data faster than the receiver can receive the data, so the sender might be sending the data faster than the intermediate switching devices (switches and routers) can forward the data, also causing discards. Packet can be lost due to transmission error as well. This happens in every network- temporarily or regularly. The receiving computer can have insufficient buffer space to receive the next incoming frame, or possibly the CPU is too busy to process the incoming frame.

Flow control attempts to reduce unnecessary discarding of data. Without flow control; some PDUs are discarded. With flow control, the sender can be slowed down enough that the original PDU. Flow-control protocols do not prevent the loss of data due to congestion; these protocols simply reduce the amount of lost data, which in turn reduces the amount of retransmitted traffic, which hopefully reduces overall congestion.

The following three methods of flow control are discussed in detail in this subsection:

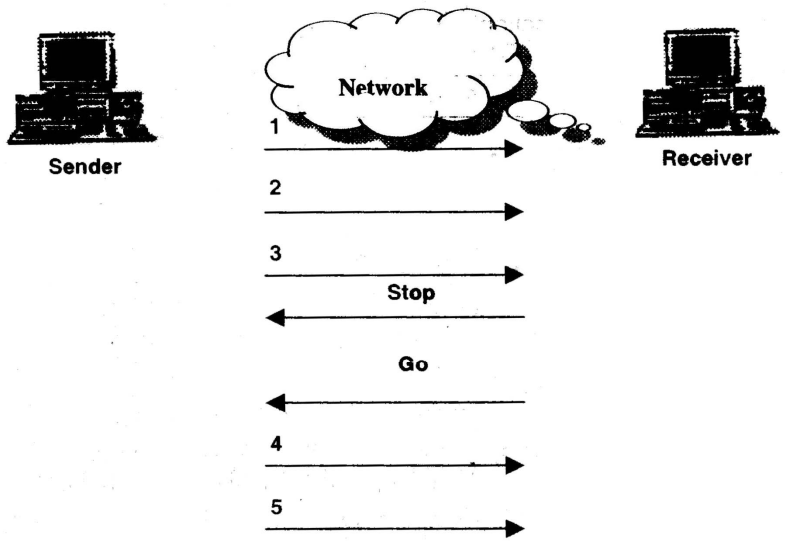
• Buffering • Congestion avoidance • Windowing

Buffering

Buffering simply means that the computers reserve enough buffer space that bursts of incoming data can be held until processed. No attempt is made to actually slow down the transmission rate of the sender of the data.

Congestion Avoidance

Congestion avoidance is the second method of flow control covered here. The computer receiving the data notices that its buffers are filling. This causes either a separate PDU, or field in header, to be sent toward the sender, signaling the sender to stop transmitting

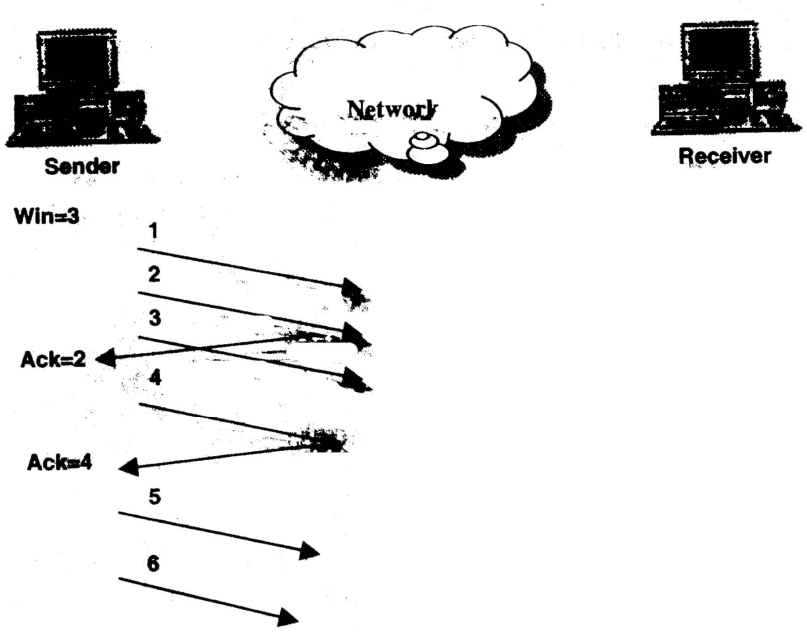


"Hurry up and waif is a popular expression used to describe the process used in this congestion avoidance method. This process is used by synchronous Data Link Control (SDLC) and Link Access Procedure, balanced serial data link protocols.

A preferred method might be to get the sender to simplify slow down instead of stopping altogether. This method would still be considered congestion avoidance, but instead of signaling the sender to stop, the signal would mean to slow down. One example is the TCCP/1P Internet Control Message Protocol (ICMP) message "Source Quench". This message is sent by the receiver or some intermediate router to sloe the sender. The sender can slow down gradually until" Source Quench" messages are no longer received.

Windowing

The third category of flow-control methods is called windowing. A window is the maximum amount of data the sender can send without getting an acknowledgement. If no acknowledgment is received by the time the window is filled, then the sender must wait for acknowledgement. The following figures shown an example.



in this example, the sender has a window of three frames. After the receiver acknowledges the receipt of frame 1, frame 4 can be sent. After a time lapse, the acknowledgement for frames 2 and 3 are received, which is signified by the frame sent by the recent, which the acknowledgement field equal to 4. so, the sender is free b send two more frames-frames 5 and 6-before another acknowledgement is received.

The following table summarizes the flow control methods and provides examples of each type.

Flow control method	Example Protocols
Buffering	Not applicable
Windowing	CFV.SPX, LLO2

7.6 SUMMARY

- ✓ The network layer is concerned with getting packets from the source all the way to the destination. Thus the network layer is the lowest OSI Network Layer functions

- ✓ The fourth layer is the Transport layer. It is primarily responsible for guaranteeing delivery of packets transmitted by Network layer.

7.7 CHECK YOUR PROGRESS – ANSWERS

7.1-7.3.1

1)
   1) Routing, Addressing & Switching
   2) Route Selection
   3) Routing Protocol

2)

1. The main purpose of network layer is concerned with getting packets from the source all the way to the destination. Getting to the destination may require making many hops at intermediate routers along the way.
2. Difference between Data Link later and Network layer transmission.
   The primary objective of the network layer is to move data to specific network locations. The layer describes methods for moving information between multiple independent networks (Internetworks). Data link layer use Addressing for it's functioning whereas Network layer uses Switching methods for it's functioning.
3. The second step in routing deals with delivering data from the router source to a router near the destination.
4. Route' selection is the ability to determine which route will be the most efficient to use to forward data to its final destination.

7.3.2 & 7.3.3

1. **Internet Address-:** Each machine on a network is- given a unique 32-bit address called as Internet address or IP address.
2. **Classes-** IP addresses are divided in to five categories, called as Network classes.
3. **Switching-:** Switching is the method of moving data through a network where multiple redundant paths exist between the source and destination.
4. **Circuit Switching-:** Circuit Switching establishes a dedicated path arid well-defined bandwidth, Which remains fixed for the duration of the connection.

7.4 & 7.5.1

1. Transport layer is primarily responsible for guaranteeing delivery of packet transmitted by the Network layer. The layer is designed to hide the characteristics of the computer network structure from the upper-layer process. It organizes-higher-level messages into segments and reliably delivers segments to session, or higher layer processes.
   The transport layer often compensates for lack of reliable, or connection oriented, connection services in the lower layers. Transport layer protocol implementations can usually confirm or deny data delivery.

2. Connection-oriented protocol-:

A protocol that either requires an exchange of messages before data transfer begins or has a required pre-established correlation between two end points

Connectionless protocol-:

A protocol that does not require an exchange of messages and that does not require a pre-established correlation between two endpoints.

Functions of Transport Layer

- Error Recovery
- Flow control

7.8 QUESTIONS FOR SELF – STUDY

1. What is the main purpose of OSI Layer 3?
2. How long is a tick?
3. Explain different types of routing protocols?
4. What is IP address?
5. Which layer protocol defines IPX address
6. Explain the routing steps involved in Network Layer?
7. What is a function of OSI layer 4?
8. Describe the features required for a protocol to be considered connectionless?
9. Which of the protocols provides error recovery?
10. What does the term reliability mean at the Transport Layer?

7.9 SUGGESTED READINGS

1. Computer Networks : Andrew Tanenbaum
2. Local Area Networks : Keiser / D. Corner

❄❄❄

NOTES

Chapter 8

OSI-Session, Presentation and Application Layer

8.0 OBJECTIVES

After studying this chapter you will be able to-

- ✓ Explain the basic purpose of the OSI Session layer.
- ✓ Describe the networking technology topics associated with the OSI Session Layer.
- ✓ Describe the methods associated with each OSI Session layer topic.
- ✓ Describe dialog control methods and session administration
- ✓ Describe purpose of Presentation Layer
- ✓ Describe purpose of Application Layer

8.1 INTRODUCTION

In this chapter we are discussing session layer, presentation layer and Application layer. Session layer is fifth layer of OSI model. It communicate between service requestor and providers. Communication sessions are controlled through mechanisms that establish, maintain synchronize and manage dialog between communicating entities. Often, this the upper layers identify and connect to the services that are available on the network.

In this OSI reference model the sixth layer is the Presentation layer, this layer performs certain functions that, are requested sufficiently, often to warrant finding a general solution, rather than letting each user solve the problems. In particular unlike all the lower layer are just interested in moving bits reliably from here to there, the presentation layer is concerned with the syntax and semeiotics of the information transmitted. It is concerned with the conversion of date formats, in the form of packets, from are machine to another.

The seventh and last layer of OSI model is Application layer. It acts as the

arbiter of translator between users application and the network. It contains a variety of protocols that are commonly needed.

8.2 PURPOSE OF OSI-SESSION LAYER

The Session layer facilitates communications between service requestors, and providers. Communication sessions are controlled through mechanisms that establish, maintain, synchronize, and manage dialog between communicating entities. Often, this layer helps the upper layers identify and connect to the services that are available on the network.

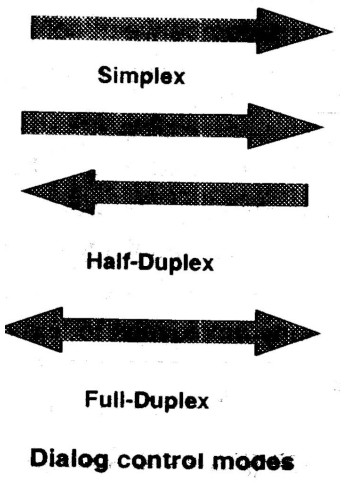
The session layer could be compared to telephone operators and telephone directory services. For example, suppose that you wanted to call a restaurant for dinner reservations but you do not know the restaurant's telephone number; you could call a telephone operator who provides directory services. That operator uses information provided by other telephone company employees to find the number of the restaurant. Similarly, the Session layer uses logical address information provided by lower layers to identify the server names and addresses that upper layers need.

After you have been told the telephone number, you could ask the telephone operator to place the call for you. The session layer also places the "calls" and initiates conversations (between service providers and requestors). When performing this function, the Session layer often Introduces' of 'identifies each of the entities and coordinates access rights.

OSI Layer	Topics	Methods
Session	Dialog Control	Simplex Full - duplex Half - duplex
	Session Administration	Connection establishment Data transfer Connection release

8.3 DIALOG CONTROL METHODS

There are three distinct dialog control modes that define the direction in which data can flow: simplex, half-duplex and full-duplex.



Dialog control modes

8.3.1 Simplex Dialog

Simplex dialog allows communications on the transmission channel to occur in one direction. Only one device is allowed to transmit: all other devices simply receive. The channels full bandwidth is always available for single travelling from the transmitter to the receiver (s). On a simplex channel, the transmitting device cannot receive information, and the receiving device(s) cannot transmit Eg- Commercial broadcast radio and television stations use simplex channels.

Simplex communications benefits and consideration:

Benefits	Considerations
Inexpensive hardware	One - way communication only
No channel contention	
Broad area coverage	
Large target audience	

8.3.2 Half-Duplex Dialog

Using half - duplex dialog, each device can both transmit and receive, but only one device can transmitting at a time. The channel's full bandwidth is available to the transmitting device (which cannot receive while is transmitting.) Use of the channel b*y* one device is limited by use of the other devices. Eg- Citizen's band radio and may LAN data transmissions use half-duplex channels. Police wireless communication equipments

Half-duplex benefits and consideration

Benefits	Considerations
Requires only one channel for both transmission and reception.	Only one unit can transmit at a time.
Bi-directional Communication is possible.	Relatively more expensive hardware than simplex
	Channel not effectively used while waiting for direction change

8.1 to 8.3.2 Check your progress.

1 . What is session of administration?

……

……

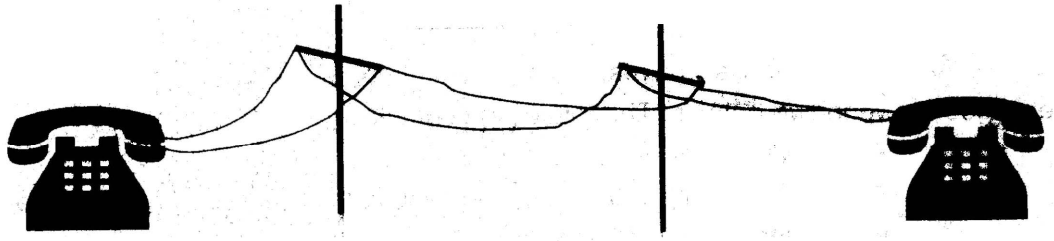
2. Explain the half duplex dialog in session layer?

……

……

8.3.3 Full-Duplex Dialog

A full-duplex Dialog allows every device to both transmit and receive simultaneously. Full-duplex communications require that every device (normally only Two) have two physical or logical transmission channels, one for receiving.



Full-Duplex Dialog

E.g.- Modern Telephone systems Provide full-Duplex Channels

Full-duplex benefits and considerations

Benefits	Considerations
Both ends can transmit at the same time	Hardware mom expensive relative to, simplex and half-duplex
	Requires more transmission media (or broadband hardware and/or software).
	Only limited or exclusive target audience available

8.4 SESSION ADMINISTRATION

As previously stated, the Session layer assists service requestors and providers lay establishing and maintaining communications in practice, this function can be split into three tasks:

- Data transfer
- Connection release

8.4.1 Connection Establishment

As its name suggests, connection establishment includes all of the subtasks that need to be performed so that the entities recognize each other and agree to communicate, Often these subtask include the following :

- Verifying, user login names and passwords
- Establishing connection identification numbers
- Agreeing which serves, are required and for what duration
- Coordinating acknowledgment numbering and retransmission procedures

8.4.2 Data Transfer

Data transfer tasks maintain the connection or communication and pass messages between two entities. The following subtasks are often performed.

- Actual data transfer
- Acknowledgment of data receipt (including negative acknowledgment when data is not received).
- Resumption of interrupted communications

8.4.3 Connection Release

Connection release is the task of ending a commutation session. It can be done by agreement between the two entities, similar to when two people say good-bye to end telephone conversation, or by an obvious loss of connection, as when one person accidentally hangs up the telephone. Entities recognize a loss of connection when they do not receive an acknowledgement or negative acknowledgement that they expect, the -service requestor (or provider) can then rebuild, the session or restart 9omrifiunications using a new session.

Check your progress - 8.3.3. to 8.4.3

1. What is Session administration?

   ……

   ……

2. What is difference between simplex and half duplex dialog?

   ……..

   ……..

3. What are the subtasks include in connection establishment?

   ……..

   ……..

8.5 PURPOSE OF THE PRESENTATION LAYER

In the OSl reference model the sixth layer is the Presentation Layer, this layer performs certain functions that are often requested sufficiently to warrant finding a general solution for them. Rather than letting each user solve the problems. In particular, unlike all the lower layers, which are just interested in moving bits reliably from here to there, the presentation layer is concerned with the syntax and-'semantics of the information transmitted.

The layer is primarily concerned with the conversion of data formats, in the form of packets, from one machine to another. The Presentation layer is responsible for picking up differences such as these and translating them to compatible formats.

The typical example of presentation service is encoding data in a standard agreed way. Most user programmes do not exchange random binary bit strings. They exchange things such as people's names, dates, amount of money and invoices. These items are represented as character strings, integers, floating point numbers, and data structures composed of several simpler items. Different computers have different- codes for representing character strings (e.g. ASCII and Unicode)integers and so on; In order to make it possible for computers with different representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with standard encoding to be used " on the wire". The presentation layer manages this abstract data1 structures and converts from the representations used inside the computer to the network standard representation and back.

8.6 PURPOSE OF APPLICATION LAYER

The seventh and last layer of OSI model is the Application Layer .it acts as the arbiter or translator between users application and the network It contains a variety of protocols that are commonly needed. For example, there are hundreds of incompatible terminal types in the world. Consider the plight of a full screen editor that is supposed to work over a network with many different terminal types, each with different screen layouts, escape sequence for inserting and deleting text, moving the cursors, etc.

One way to solve this problem is to define an abstract Network virtual terminal that editors and other programs can be written to deal with. To handle each terminal type, a piece of software must be written to map the functions of the network virtual terminal onto the real terminal. For example when the editor moves the virtual terminal's cursor to the upper left-hand comer of the screen, this software must issue

the proper command sequence to the real terminal to get its cursor too. All the virtual terminal software is in the application layer.

Another Application layer function is file transfer. Different files systems have different file naming conventions, different ways of representing text lines, and so on. Transferring a file between two different systems requires handling these and other incompatibilities. This work too, the application layer, as do electronic mail, remote job entry, directory lookup, and various other general-purpose and special-purpose facilities.

8.7 SUMMARY

In this chapter we studied

- ✓ The session layer facilities communication between service requestors and providers. Communication sessions are controlled through mechanisms .that establish, maintain synchronize, and manage dialog between communicating entities.
- ✓ Session layer functions with the following methods
  - Dialog Control
  - Session Administration
- ✓ In the OSI reference model the sixth layer is the Presentation Layer, this layer performs certain functions that, are requested sufficiently, often to warrant finding a general solution. Rather than letting each user solve the problems. In particular unlike all the lower layer which are just interested in moving bits reliably from here to there the presentation layer is concerned with the syntax and semantics of the information transmitted.
- ✓ The seventh and last layer of OSI model is the Application Layer. It acts as the arbiter or translator between users application and the network. It contains a variety of protocols that are commonly needed.

8.8 CHECK YOUR PROGRESS – ANSWERS

8.1 to 8.3.2

1. The session layer facilities communications between service requestors and providers. Communication sessions are controlled through mechanisms that establish, maintain, synchronize, and manage dialog between communicating entities. Often, this layer also help the upper layers identify and connect to the services that are available on the network.
2. Using half - duplex dialog, each device can both transmit and receive, but only one device can transmitting at a time.

   Advantages : Requires only one channel for both transmission and reception Bi-directional Communication is possible.

8.3.3 to 8.4.3

1. For facilitating the communication between service requestor and providers, communication sessions are controlled through connection establishment; Data transfer ands connection release is called as Session administration.
2. Simplex dialog allows communication on the transmission channel to occur in one direction, whereas in Half-duplex, each device can both transmit and receive, but only one device can transmitting at a time.
3. Following Sub-tasks are include in Connection establishment :

- Verifying user login names and passwords
- Establishing connection identification numbers
- Agreeing which services are required for what duration
- Determining which entity begins the conversation
- Coordinating acknowledgment numbering and retransmission procedures

8.9 QUESTIONS FOR SELF – STUDY

1. What is function of OSI-Session Layer
2. Explain the different methods of dialog control with proper example?
3. What is connection establishment?
4. What do you mean by session administration?
5. Explain OSI-Application Layer in detail?
6. What is a purpose of OSI-Presentation Layer?
7. What is data transfer?

8.10 SUGGESTED READINGS

1. Computer Networks : Andrew Tanenbaum
2. Computer Networks : A Top Down Approach by Behrouz forouzan mosharraf

❄❄❄

NOTES

Chapter 9

TCP/IP Fundamentals

9.0 OBJECTIVES

After studying this chapter you will be able to-

- ✓ Explain what is internet Protocol Stack
- ✓ Describe what is TCP/IP
- ✓ Discuss advantages of TCP/IP
- ✓ State purpose of Layers
- ✓ Discuss different types of Network Classes
- ✓ Explain different services installed with TCP/IP Protocol
- ✓ Explain configuration of IP address and subnet mask

9.1 INTRODUCTION

As discussed earlier, you are familiar with computer networks, transmission media as well, as seven layers of OSI model. Network is nothing but group of two or more computer systems sharing services and interacting in some way. But for this interaction you need some physical pathway (transmission media). This transmission media connects the systems, and a set of rules determines how they communicate. These rules are known as protocol. A network protocol is software installed on machine that determines the agreed-upbn set of rules for two or more machines to communicate with each other.

Common protocols in the Microsoft family include the following.

- NetBEUI
- NWLink
- DLC (Data Link Control)
- TCP/IP (Transmission Control Protocol / Internet Protocol)

In order to understand how to configure the functions of network devices, you must have a solid understanding of the protocols and their functions. The most common protocol used; in data networks today is the TCP / IP protocol stack. TCP/IP is used to interconnect devices in corporate networks as well as being the protocol of the Internet. The TCP/IP suite of protocols was developed as part. of the research

done by the Defence Advance Research Projects Agency (DARPA). Later TCP/IP was included with the Berkeley Software Distribution (BSD) UNIX. TCP/IP is an industry-standard suite of protocols designed to be routable, robust, and functionally efficient.

The Internet protocols can be used to communicate across any set of Interconnected networks. They are equally well suited for both LAN and WAN communication the Internet protocol suite includes not only Layers 3 and 4 specifications, but also specifications for such common applications as e-mail, remote login, terminal emulation, and file transfer. The TCP/IP protocol stacks maps closely to the OSI reference model in the lower layer. All standard Physical and data-link protocols are supported.

Installing TCP/IP as a protocol on your machine or network provides the following advantages :

1. An industry-standard protocol

Because TCP/IP is not maintained or written by one company, it is not subject to as many compatibility issues. The Internet community as whole decides whether a particular change or implementation is worthwhile. This slows down the implementation of new features and characteristics compared to how quickly one directed company might make changes, but it does guarantee that changes are well thought out, that they provide functionality with most other implementations of TCP/IP.

2. As set of utilities for connecting dissimilar operating systems

Many connectivity utilities have been written for the TCP/IP suite, including the Pile Transfer Protocol (FTP) and Terminal Emulation Protocol (Telnet). Because these utilities use the windows Sockets API, connectivity from one machine to another is not dependant on the network operating system used on either machine.

3. A scalable Cross-platform client-server architecture

4. Access to the Internet

TCP/IP is the de facto protocol of the Internet and allows access to a wealth of information that can be found at thousands of locations around the world. To connect to the Internet, a valid IP address is required. Because IP address have become more and more scare, and as security issues surrounding access to the Internet have been raised, many creative alternatives have been established to allow connections to the internet.

Now you understand the benefits of installing TCP/IP, you are ready to team about how the TCP/IP protocol suite maps to a four -layer model.

OSI	TCP/IP
Application	Application
Presentation	
Session	Application
Transport	Transport
Networking	internet
Data Link	Network interface

Physical

TCP/IP maps to four layer architectural model. This model is called the Internet protocol suite and is broken into the network interface, Internet, Transport, and Application layers. Each of these layers corresponds to one or more layers of the OSI model. The Network Interface layer corresponds^*lo* the Physical and Date Link layers. The Internet layer corresponds to Network layer. The transport layer corresponds to the transport and application layer corresponds to the Session, Presentation, and Application layer.

9.2 PURPOSE OF LAYERS (TCP/IP MODEL)

The Network Interface layer is responsible for communicating directly with the network. The Internet layer is primarily concerned with the routing and delivery of packets through the Internet protocol (IP). All protocols in transport layer must use IP to send data.

The transport layer maps to the Transport Layer of OSl model and is responsible for providing communication between machines for applications.

The Application layer of the Internet Protocol Suite is responsible for all the activities that occur in the session, presentation an application layer of the OSI model. Numerous protocols have been written for use in this layer, including HTTP, Simple Network Management Protocol SNMP File Transfer Protocol (FTP) etc.

9.1 & 9.2 Check your progress

Answer in brief.

1. What are the advantages of TCR/IP protocol?

   ……..…….

   ……

2. List the layers inducted in TCP/IP Model.

   ……..…….

   ……..…….

9.3 NETWORK CLASSES

In a TCP/IP environment, end stations communicate seamlessly with servers or other end stations. This communication occurs because each node using the TCP/IP protocol suite has a unique 32-bit logical IP address. These addresses are called as Network classes. Each IP diagram includes a source IP address and destination IP address that identify the source and desolation network and host.

There are currently A, B, C, D and E classes of addresses. The unique address given to a machine is derived from the class A, B, or C addresses. Class D addresses are used for combining machines into one functional group, and class E addresses are considered experimental and are not currently available. For now, the most important concept to understand is that each machine requires a unique address and that IP is responsible for maintaining, utilizing, and manipulating it to provide communication between two machines. The whole concept behind uniquely identifying machines, is to be able to send data to one machine and one machine only, even in the event that the IP stack has to broadcast at the physical layer.

Term	Definition
Default Mask Class A	The mask used for class A network when no subnetting The value is 255.0.0.0
Default Class B Mask	The mask used for class B network when no subnetting is used. The value is 255.255.0.0
Default Class C Mask	The mask used for class A network when no subnetting is used. The value is 255.255.255.0

When IP was first developed, there were no classes of addresses, because it was assumed that 254 networks would be more than enough for an Internet of academic and research computers. As the number of networks grew, the IP addresses were broken into classes as illustrated in the figure given below.

	8 Bits	8 Bits	8 Bits	8 Bits
Class A:	Network	Host	Host	Host
Class B :	Network	Network	Host	Host
Class C :	Network	Network	Network	Host
Class E :	Multicast Research			

Class A address has only 8 network bits (1 byte) and 24 bits (3 bytes) in the host field. Therefore, few Class A networks, each consisting of many hosts, exist. There are more Class B and Class C networks, each with fewer hosts. This scheme allows addresses to be assigned based on the size of network. This address design was based on assumption that there would be many more small networks than large networks in the world.

Characteristics of Class A, B and C addresses

Class A Address	Class B Address	Class C Address
The first bit is 0.	The first two bits are 10.	The first three bits are 110.
Range of network numbers: 1.0.0.0 to 126.0.0.0	Range of network numbers: 128.0.0.0 to 191 .255.0.0	Range of network numbers: 92.0.0.0 to 223.255.255.0
Number of possible networks: 127 (through 126 are usable127 is reserved)	Number of possible networks 116,384	Number of possible networks: 2,097,152
Number of possible values host portion : 16777,216 (the number of usable hosts is two less than the total number possible because the host portion must be nonzero and cannot be all 1s.)	The number of possible values in the Host portion : 65,536 (the number of usable hosts is two less than the total number possible because the host portion must be nonzero and cannot be all 1s.)	The number of possible in the values in the host portion : 256 (the number of usable hosts is two less than the total number possible because the host portion must be nonzero and cannot be all 1 s.)

Class D and Class E addressee are also defines. Class D addresses include the range of networks numbers: 224.0.0.0 to 239.255.255.255.Class E addresses start at 240.0.0.0 and are used for experimental purposes.

When installing the TCP/IP protocol, you have, the choice of installing and using several different services that work in conjunction with it. You may want or need to install the following services.

- **Internet Information Server (IIS)**

The Internet Information Server provides you the ability to share information to any type of computer that can use the TCP/IP protocol. IIS 3 includes FTP and WWW servers

- **Dynamic Host Configuration Protocol (DHCP)**

Provides automatic configuration remote hosts, making management of a TCP/IP environment easy.

- **Windows Internet Name Service**

Without the ability to find another computer on the network, you would never be able to communicate .The WINS server provides a centralised method of name management that is both flexible and dynamic in Microsoft only network.

- **Domain Name Server**

When the WINS server provides the capability to find the NETBIOS names, the DNS server will work with host names to enable you to integrate your systems into the Internet or to resolve hosts on the Internet.

9.4 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

The configuration of Microsoft TCP/IP involves knowing the correct values for several fields for each TCP/IP host and entering them manually. At the minimum, the host IP address and the subnet mask need to be configured. In most cases, other parameter such as WINS and DHCP server addresses also need to *be* configured on each host. DHCP relives the need for manual configuration and provides a method of configuring and reconfiguring all the TCP/IP related parameters. It is critical that the correct TCP/IP address is configured on each host.

The use of Microsoft's DHCP server greatly reduces the administrative overhead of managing TCP/IP client computers by eliminating the needs to manually configure clients. The DHCP server also allows for greater flexibility and mobility of clients on a TGP/IP network without administrator intervention. If used correctly DHCP can eliminate nearly all the problems associated with TCP/IP. The administrator enters the valid IP addresses or ranges of IP addresses (called a scope) in the DHCP server database, which then assigns the IP addresses to the DHCP client hosts.

9.5 DOMAIN NAME SYSTEM

The Domain Name System is one way to resolve hostnames in IP addresses in a TCP/IP environment. In non-Microsoft environment, hostnames are typically resolved through HOST files or DNS. In a Microsoft environment, WINS and broadcasts are also used to resolve hostnames on the Internet.

In it's early days, the Internet was a small network established by the Department of Defence for research purposes. This network linked computers at

several government agencies with a few universities. The host names of the computers in this network were registered in a single HOSTS file located on a centrally administered server. Each site that heeded to resolve hostnames downloaded ^his file. Few computers were being added to this network, so the HOSTS file was not updated too often and the different sites only had to download this file periodically to update their own copies. As the number of hosts on the Internet grew, it becomes more and more difficult to manage all the names through a central HOSTS file.

DNS was introduced in 1984 as a way to resolve hostnames without relying on due central HOSTS file. With DNS, the hostnames reside in a database that can be distributed among multiple servers, decreasing the load on any one server and also allowing more than one point of administration for this naming system. DNS allows more types of registration than the simple hostname-to-TCP/IP address mapping used in

HOSTS files and allows room for future-defined types. Because the database is distributed, it can support a much larger database that can store in single HOSTS file.

9.5.1 Structure of DNS

Some hostname systems, like NetBIOS names, use a flat database. With a flat database, all names exist at the same level, so there cannot be any duplicate names. These names are like Social Security numbers: every participant in the Social Security program must have a unique number, so it must be an identification system to distinguish all the individuals in the security. DNS names are located in hierarchical paths, like a directory structure. In a network using DNS, you can have more than one server with the same name, as long as each is located in a different path.

9.5.2 DNS Domains

The Internet Network Information Center Controls the top-level domains. These have names such as "com", "edu", ‘Gov’, "org" etc.

Name	Type of organization
Com	Commercial organizations
Edu	Educational institutions
Org	Non-profit organizations
Net	Networks
Gov	Non-military government organizations
Num	Phone numbers

The DNS database is stored in a file called zones. It is possible, even desirable, to break the DNS database into a number of zones. Breaking the DNS database into zones was part of the original

9.3 to 9.5 Check your progress.

1. Define IP address?

   ……

   ……

2. What are the characteristics of class A?

   ……

   ……

3. What type of services, we can install with TCP/IP protocol?

   ……

   ……

4. What is DHGP?

   ……

   ……

5. What is DNS?

   ……

   ……

9.6 WINDOWS INTERNET NAME SERVICE

WINS is used to map NetBIOS (computer) names to IP addresses dynamically. The main function can be performed in the absence of a WINS server with LMHHOSTS files, but the files are static and do hot incorporate changes. The only time a WINS server automatically collects entries is when a WINS, client is configured with that WINS server's address. When the client starts up, it sends are registration request to the WINS server. After a client registers its NetBIOS name with a WINS server, it is the client's responsibility to renew the registration. The WINS server does not initiate any registration renewals with clients. The registration is released if not renewed by the time the TTL expires.

You can also enable non-WINS clients to use a WINS server to resolve NetBIOS names by installing a WINS proxy agent. By definition, a non-WINS client cannot directly communicate with a WINS server to resolve a name. The non-WINS client resolves names by restoring to a b-node broadcast. If you install a WINS proxy agent, the proxy agents' forwards any broadcasts for name resolution to the WINS server. The proxy agent must be located on the same subnet as non-WINS clients so that proxy agent receives the Broadcast for name resolution.

You must place a WINNS proxy agent on each subnet where non-WINS clients are located so that those clients have access to the WINS server.

9.7 IP ADDRESS

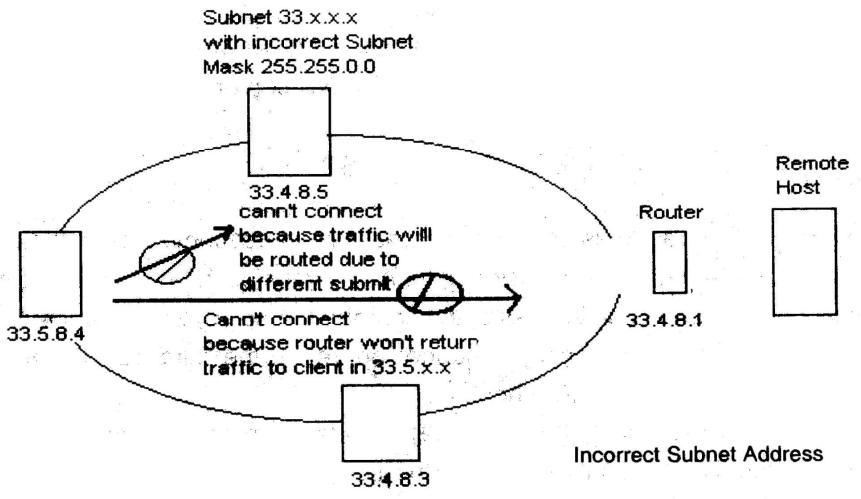
A TCP/IP address has two or possibly three components that uniquely identify the computer the address assigned to. At the very least, the IP address specifies the network address and host address of the computer. Also, if you are subnetting (using part of the host address to specify a subnet address), the third part of the address

specifies the subnet address of the host.

If the incorrect host (143.168.3.9) sends a message to a local client (133.168.3.20 the TCP/IP configuration of the pending host indicates this is a remote address because it doesn't IP match the network address of the -host initiating the communication. The packet will not reach the local client, because the address 133.168.3.20 is interrupted as remote address.

If a local client the incorrect host (143.168.3.9), the message never reaches its intended destination. The message is either routed (if the local client sends the it to what should have been the address, 133.168.3.9). If the message is routed, the routed, the client for whom it was intended cannot receive the message because it is on the same segment of the network as the local client. If the message is not routed, the message still does not reach the incorrect client because the IP address for the destination host (133.168.3.9) does not match the address as configured on the incorrect client (143.168.3.9).

Following figure gives an example of an incorrect IP address. In this case a class A address is used, 33.x.x.x. The subnet mask (255.255.0.0) indicates the second octet is also being used to create subnets. In this cases even though the client has the same network address as the other clients, on the same subnet, the client has a different number because the address was typed incorrectly. This time the incorrect address specifies the Wrong subnet ID. The client 33,5.8.4 is on subnet 5, but the other clients on this subnet have the address 33.4.x.x. In this case, if the client 33.5.3.4 tries to contact other clients on the same subnet, the message is pouted because the subnet ID does not match the subnet number of the source host. If the client 33.5.8.4 tries to send a message to a remote host the message grouted but the message is not returned to the client because the router doesn't handle subnet 5, only subnet 4.

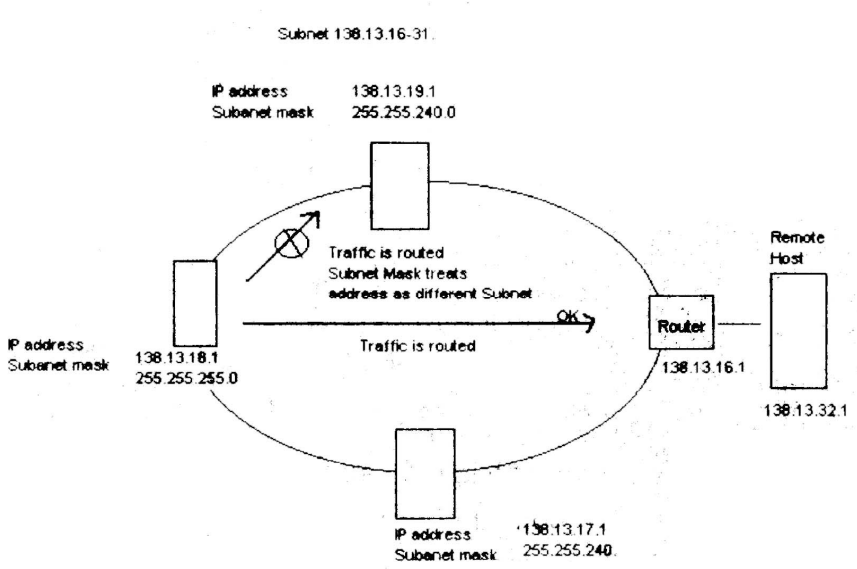


If a local client tries to send a message to 33.5.8.4, the message does not reach the client. If the local client uses the address as configured, the message is routed, which is not the correct solution because the destination host is local. If the local client sends the message to what should have been the IP address, 33.5.8.4 does not receive the message because the IP address is not configured correctly. The last component of an IP address that can cause communication problems in the host address.

9.8 SUBNET MASK

The subnet mask specifies which portion of the IP address specifies the network address and which portion of the address specifies the host address. Also, the subnet mask can be used to take part of what would have been the host address and use it to further divide the network into subnet. If the subnet mask is not configured correctly, yours client may not be able to communication at all, or you may see partial communication problems.

The following figure shows a subnet on a TCI/IP network. It uses a Class B network address of 130.13.x.x. The third octet is used in this case for subnetting, however, so all the clients in the figure should be on subnet 4, as indicated by the common address 138.13,3.x. Unfortunately, the subnet mask entered for one client is 255.255.0.0. When this client tries to communicate with other hosts on the same subnet, it should be able to contact them because the subnet mask indicates they are on the same subnet, which is correct. If the client tries to contact a host on another subnet such as 138.13.3.x, however the client fails.

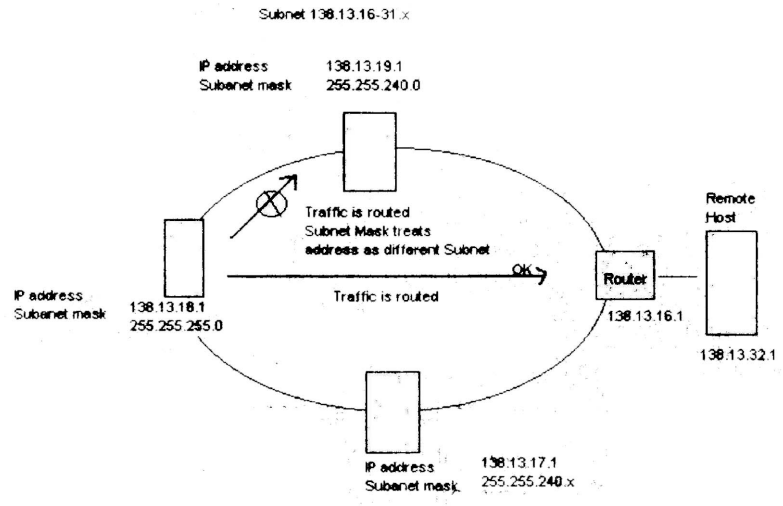


Incorrect subnet mask-missing third octet

In this case, the subnet mask still interprets the destination host to be on the same subnet and the message is never routed. Because the destination host is on another subnet, the message never reaches the intended destination.

The subnet mask is used to determine whether the host is local or remote, so the client with the incorrect subnet mask can receive incoming messages. When the client tries to return communications, however, the message is not routed if the source host is on the same network but on a different subnet. So in actuality, the client really can establish communications with only one side of the conversation. Contact with hosts outside the local network still works because those contacts are routed.

The following figure shows a subnet mask that masks too many bits. In this case, the subnet mask, is 255:255.255.0. The network designers had Intended the subnet mask to be 255.255.240.0, however, with 4 bits of the third octet used for the subnet and 4 bits as part of the host address. If the incorrect client tries to send a message to a local host and third octet is the same, the message is not routed and therefore reaches the local client, if the local client has an address that differs in the last 4 bits<of the third octet, however, the message is routed and never reaches its destination. If the incorrect client tries to send a message to another client on another subnet, the message is routed because the third octet is different.



9.9 SUMMARY

In this chapter we studied

- ✓ Network is nothing but group of two or more computer systems sharing services and interacting in some way. But for this interaction you need some physical pathway (transmission media). This transmission media connects the systems, and a set of rules determines how they communicate. These rules are known as protocol. A network protocol is software installed on machine that determines the agreed upon set of rules for two or more machine to communicate with each other.

- ✓ Common protocols in the Microsoft family include the following.

  1.NetBEUI

  2. NWLink

  3. DLC (Data Link Control)

  4. TCP/IP (Transmission Control Protocol /internet protocol)

- ✓ In a TCP/IP environment, end stations communicate seamlessly with servers and other end stations. This communication occurs because each node using the TCP/IP protocol suite has a unique 32-bit logical IP address. These addresses are called as Network classes.

- ✓ There are currently A, B, C, D and E classes of addresses. The unique address given to a machine is derived from the class A, B, or C addresses. Class D addresses are used for combining machines into one functional group, and class E addresses are considered experimental and are not currently available.

  Default Class A Mask- The mask used for Class A network when no sub netting is used. The value is 255.0.0.0

  Default Class B Mask- The mask used for class B network when no subnetting is used. The value is 255.255.0.0

  Default Class C Mask- The mask used for Class A network when no subnetting is used. The value is 255:255.255.0

.

Sources : *pluto.ksi.edu, http://www.techiwarehouse.com (Link)*

9.10 CHECK YOUR PROGRESS – ANSWERS

9.1 – 9.2

1. Advantages of TCP/IP protocol
   - An industry-standard protocol
   - As set of utilities for connecting similar operating systems
   - A scalable. Cross-platform client-server architecture
   - Access to the Internet
2. Following layers are included in the TCP/IP model-
   - Application ,
   - Transport
   - Internet
   - Network interface

9.3 – 9.5

1. IP address-: Each machine on a network is given a unique 32-bit address called as IP address.
2. Characteristics of Class A-
   - The first bit is 0.
   - Class A networks ranges from 1.0*0.0 to 126.0.0,0
   - Total 127 networks can possible with class A
   - Number of possible values in the Host portion: are 16777,216
3. Following services we can install with TCP/IP protocol.
   - Internet Information Server (US)
   - Dynamic Host Configuration Protocol (DHCP
   - Windows Internet Name Service
   - Domain naming service.
4. DHCP is "Dynamic Host Configuration Protocol" which Provides automatic configuration of remote hosts, making management of a TCP/IP environment easy.
5. DNS is "Domain Name System" which resolves hostnames in IP addresses in a TCP/IP environment.

9.11 QUESTIONS FOR SELF – STUDY

1. Explain the role of DHCP?
2. What is use of WINS server?
3. Explain subnet mask in detail?
4. List the advantages of TCP/IP?
5. Write a note on Network Glasses?
6. Write the characteristics of Network Class C?
7. What type of services we can install with TCP/IP?
8. Explain how to configure IP address?

9.12 SUGGESTED READINGS

1. Computer Networks : Andrew Tanenbaum
2. Computer Networks : A Top Down Approach by Behrouz forouzan mosharraf

❁❁❁

Chapter 10

Windows XP

10.0 OBJECTIVES

After studying this chapter you will be able to-

- ✓ Explain basic concept of operating system of Multitasking.
- ✓ Explain Windows XP.

10.1 INTRODUCTION

An Operating system is a part of system software that is loaded in to computer on boot up that is responsible for running other applications and provides interface to interact with other programs that uses system hardware.

This interface is either command line user interface or Graphical User Interface. Command Line User interface is used in operating systems like MSDOS, UNIX, LINUX etc. and GUI is used with most of MS Windows operating systems like Windows XP , Windows Vista Windows 7 etc.

Operating system can be divided into two groups : 1] Single process & 2] Multi process.

Single process operating systems are capable of working on one task at a time while multi process operating systems can work on several processes at once by breaking the tasks into threads. Smallest part of programs that can be scheduled for execution is called as a thread. There are several terms related to multiprocessing which are as follows

10.2 MULTITASKING

It is the capability of an operating system to handle more than one task at a time. There are two types of multitasking

1] Co-operative Multitasking 2] Preemptive multitasking.

1. Co-operative Multitasking

Applications can control the system resource until they are finished. If a task

caused faults or other problems, it would cause the system to become unstable and force a reboot. This type of multitasking is used in Windows 3.x.

2. Preemptive Multitasking

Applications are allowed to run for a specified period of time depending on how important the application is to the operation of the system (priority basis). If a particular task is causing problems or faults, that application can be stopped without the system becoming unstable. Used in Windows 9.x, Windows XP, Vista and Windows 7 and all network operating systems.

Multi user - This is similar to multitasking and is the ability for multiple users to access resources at the same time. The OS switches back and forth between users. For example all network operating systems like Windows server 2003, Windows server 2008, Linux, Unix etc.

Multiprocessor - Having multiple processors installed in a system such that tasks are divided between them. Now all latest operating systems uses symmetric multiprocessing.

Multiprogramming : It is the capability of an operating system to run multiple programs at once. Multiprogramming is possible because of multi threading.

Multithreading :- It is the capability of an operating system to handle (execute) multiple threads of multiple programs at a time. One program may have at least one thread. Thread is a smallest part of a program that can be scheduled for execution.

There are two broad categories of operating systems 1] Desktop operating system 2] Network operating system.

Desktop operating System:-

Features of Desktop operating system

1] It a single user operating system.
2] It can support Multitasking, Multiprogramming, Multiprocessing and Multithreading. 3] User interface can be command line or GUI.
4] Desktop PCs, workstations and laptops are used to installed desktop operating systems.
5] Cost of the operating system is low as compare to Network operating system.
6] Desktop operating system can be configured as a client in network environment.
7] Provides user level and share level security.
8] Desktop operating systems are as follows :
MSDOS, Windows 95/98, Windows 2000 Professional, Windows XP, Windows Vista and Windows 7.

10.3 WINDOWS XP STRUCTURE

Windows XP operating system is either 32 bit or 64 bit operating system that run in 2 different modes which are kernel(protected) and user. Applications use Application Program Interfaces(APIs) to pass threads between the 2 modes. User mode provides no direct access to the system's hardware.

Windows XP has various editions like Windows XP Home, Windows XP Professional, Windows XP Media Centre etc. Windows XP supports two way SMP i.e. it supports maximum two CPUs. Windows XP Home Edition does not take part in Domain Environment.

Features of Windows XP :-

Windows XP combines the features of Windows 2000 Professional, Windows 98 and Windows ME. The main benefit of using XP include its reliability, performance, security, ease of use, support for remote users, networking and communication support, management and deployment capabilities, and help and support features.

Hardware Requirements

To install Windows XP Professional successfully, your system must meet certain hardware requirements. Table 1.1 lists the minimum requirements for a *x*86-based computer, as well as the more realistic recommended requirements.

The standard Windows XP Professional operating system is based on the Intel *x*86-based processor architecture, which uses a 32-bit operating system.

Windows XP 64-bit edition is the first 64-bit client operating system to be released by Microsoft. The 64-bit version of Windows XP requires a computer with an Itanium processor, and is designed to take advantage of performance offered by the 64-bit processor. The hardware requirements for Windows XP 64-bit edition are different from the hardware requirements of a standard version of Windows XP Professional. Maximum memory supported by Windows XP is 3GB for 32 bit edition.

Note: Windows XP Professional offers support for a maximum of 2 processors and a maximum of 4 GB Ram for 64 bit edition.

Component Minimum Requirement

- Processor Intel Pentium (or compatible)
- 233MHz or higher
- Intel Pentium II (or compatible)
- 300MHz or higher
- Memory 64MB or 128MB
- Video adapter and monitor with
- SVGA resolution or higher
- Peripheral devices like Keyboard, mouse, or other pointing device
- Removable storage
- CD-ROM or DVD-ROM drive if installing from CD
- 12x or faster CD-ROM or DVD-ROM

File Systems Supported

Windows XP Professional supports three file systems:

_ File Allocation Table (FAT16)

_ FAT32

_ New Technology File System (NTFS)

While Windows XP Home Edition adds a great deal to the feature set of Windows 2000, Windows XP Professional takes the product to the next level. Many of the neat things that are part of Windows 2000 Professional are excluded from the Home Edition, but they are included in WinXP Professional. These features include the following:

- IntelliMirror technologies
- Group Policy functionality
- Encrypting file system support
- Multiprocessor support

Check your progress

Fill in the blanks

1] Windows XP operating system is either ……. bit or ……. bit operating system.

2] Windows XP operating system that run in 2 different modes which are ……. and …….

3] Windows XP supports maximum ……. CPUs.

4] Maximum memory supported by Windows XP is …….

5] Windows XP ……. edition does not take part in Domain environment.

New Features and Improvements

Automatic Updates

Windows XP Professional includes an Automatic Updates (AU) feature. AU is a proactive service that allows users with administrative privileges to automatically download and install critical operating system updates, such as security fixes and patches. Because the installation might require you to restart your computer, you are notified before the installation takes place and given the opportunity to postpone the download operation. Updates are downloaded in the background so that you can continue to work during downloading.

AU uses the Windows Update control to scan the system and decide which updates apply to a particular computer. AU uses its innovative bandwidth-throttling technology for downloads. Bandwidth throttling uses only idle bandwidth so that downloads do not interfere with or slow down other network activity, such as Internet browsing. Only one administrative user at a time can run the AU client.

Copying Files and Folders to a CD

Windows XP Professional enables users to save information such as photos and software to a compact disc (CD) without using third-party software. Because CD-recordable (CD-R) and CD-rewritable (CD-RW) drives are now inexpensive options on computers, this feature enhances the standard conveniences that Windows offers to users.

Users can select a folder of images from a digital camera, drag it to the CD-R icon, and then create a CD. They can also transfer files more easily to a CD instead of copying them to a smaller capacity floppy disk.

This feature also provides options for original equipment manufacturers (OEMs) and independent software vendors (ISVs). OEMs can create branded applications that generate emergency boot CDs instead of emergency boot floppy disks, and ISVs can offer a "burn to CD" option on their Windows versions.

To copy files or folders to a CD follow these steps:

1. Insert a blank, writable CD into the CD recorder. You must have a blank, writable CD and a CD-ROM drive that has the capability of writing CDs to use this feature.
2. Click Start, right-click My Computer and select the files and folders you want to write to the CD.
3. Under File And Folder Tasks, click Copy This File, Copy This Folder, or Copy The Selected Items.
4. In the Copy Items dialog box, click the CD recording drive and then click Copy.
5. In My Computer, click the CD recording drive and then under CD Writing Tasks, click Write These Files To The CD.

Standard CDs hold 650 MB of information. High-density CDs hold at least 700 MB of information. You must have enough space on your hard drive to temporarily hold the files you want to copy to the CD or the operation will fail.

Clear Type Support

Windows XP Professional supports Clear Type, a new text display technology. Clear Type triples the horizontal resolution available for rendering text through software, which provides a clearer text display on a liquid crystal display (LCD) screen with digital interface.

To specify Clear Type follow these steps:

1. Click Start and then click Control Panel.
2. Click Appearance And Themes, and then click Display.
3. In the Appearance And Themes dialog box, click Appearance.
4. In the Appearance tab, click Effects.
5. Select the Use The Following Method To Smooth Edges Of Screen Fonts check box, and then select Clear Type from the drop-down list (see Figure 1.1).

Figure *The Effects dialog box* 6. Click OK to close the Effects dialog box.

7. Click OK to close the Display Properties dialog box.

Compressed Folders

The Compressed Folders feature provides the ability to create ZIP folders and view their contents. Compressed folders allow you to compress large files so that you can store more files on a floppy disk or hard drive.

To create a compressed folder follow these steps:

1. Click Start, right-click My Computer, and then click Explore.
2. On the File menu, click New, and then click Compressed Folder.

If you drag and drop files and folders into a compressed folder, they will be compressed. You cannot save a file to a compressed folder.

Desktop Cleanup Wizard

The Desktop Cleanup Wizard helps keep your desktop uncluttered by periodically checking for unused shortcuts and removing them without harming the installed program. By default, the Desktop Cleanup Wizard checks for unused shortcuts every 60 days and offers to move them to a folder on the desktop called Unused Desktop Shortcuts.

To run the Desktop Cleanup Wizard follow these steps:

1. Click Start, and then click Control Panel.
2. Click Appearance And Themes, and then click Display.
3. Click Desktop and then click Customize Desktop. Windows XP Professional displays the Desktop Items dialog box, as shown in Figure 1.2.

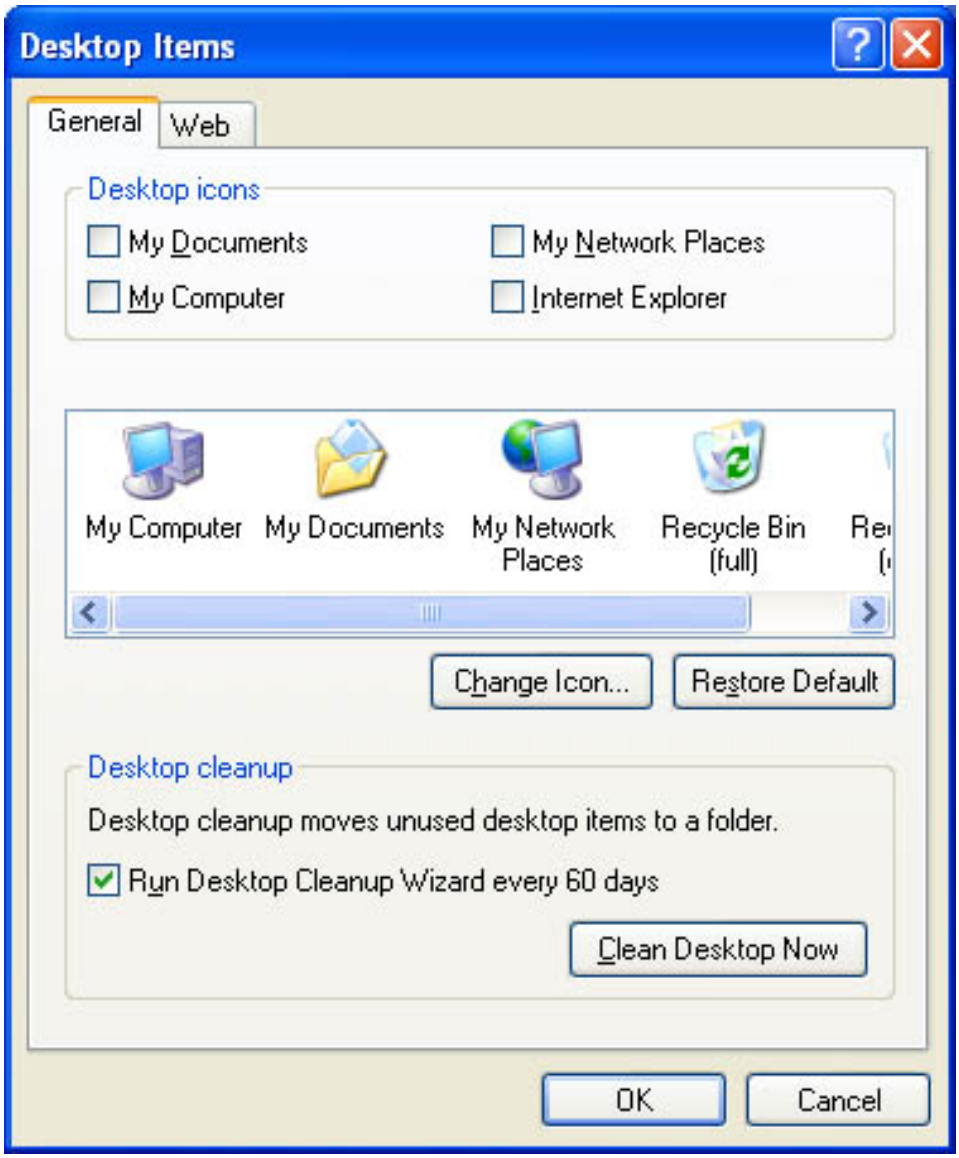


Figure *The Desktop Items dialog box* 4. Under Desktop Cleanup, click Clean Desktop Now to run the Desktop Cleanup Wizard now.

Start Menu

The Start menu has been redesigned for easier access to important and frequently used tasks. In addition to prominent Internet and e-mail links, the new Start menu lists the programs that you use most frequently. Windows XP Professional continually updates this list based on your usage of programs. It adds programs that you are using and removes programs from the list that you have not been using. Windows XP Professional does not remove the programs from your computer, just from this list. The Start menu also lists important user folders such as My Documents, My Pictures, and My Music.

To customize the Start menu follow these steps:

1. Right-click Start and then click Properties.
2. Click the Start Menu tab. The Start Menu tab lets you choose between the Windows XP Professional Start menu and the Classic Start menu used in earlier versions of Windows.
3. Click Customize. The Customize Start Menu dialog box has two tabs: General and Advanced. The General tab allows you to select an icon size for programs, configure the amount of frequently used programs you want displayed on the Start menu, and select the Internet and e-mail items shown on the Start menu. The Advanced tab, shown in Figure 1.3, allows you to configure Start menu settings, items, and recent documents.

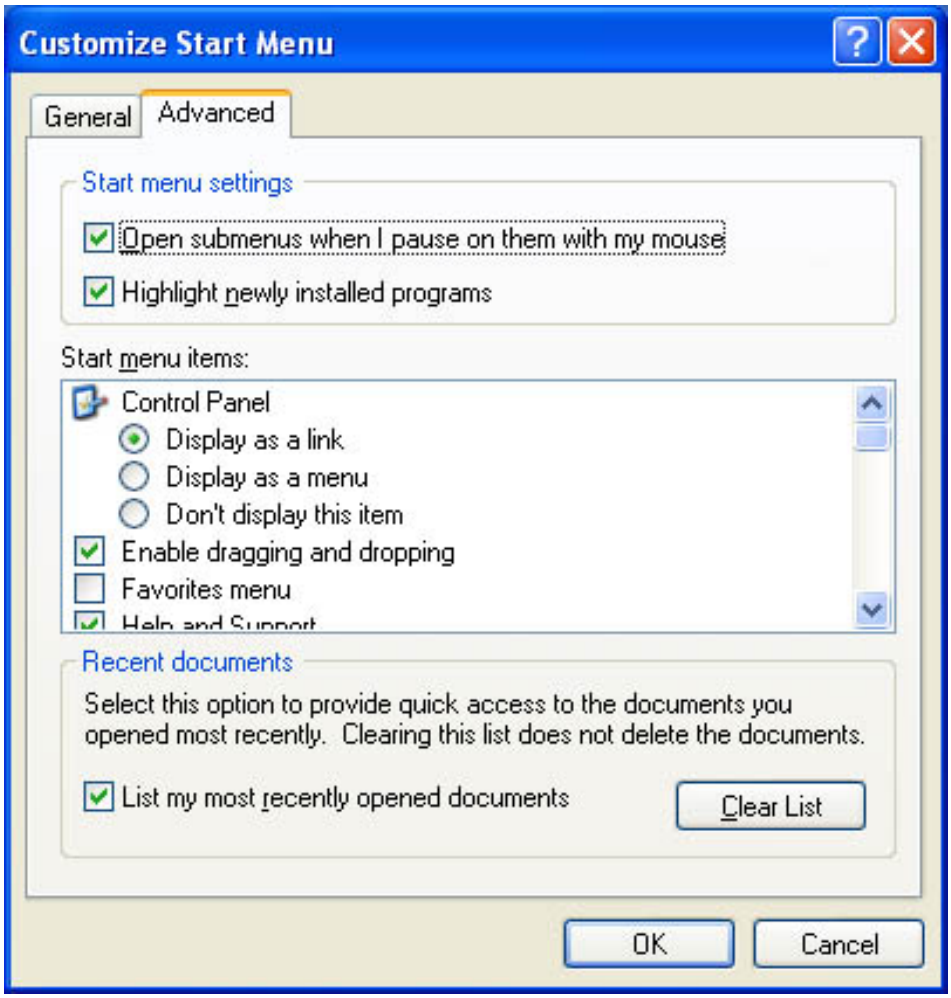


Figure *The Advanced tab of the Customize Start Menu dialog box*

Fax Support

Windows XP Professional provides fax support that enables you to send faxes over a network from a computer with an attached fax modem or fax board or with a local area network (LAN) connection. You can print to fax from any application, send cover fax pages, and track and monitor faxes. New wizards enable simpler configuration of this feature and fax sending.

IT administrators can use the Component Object Model (COM) application programming interface (API) to control fax capabilities and the Microsoft Management Console (MMC) to set up the fax service within their infrastructure. Developers can use COM to send faxes programmatically. In addition, they can use the fax APIs to write applications to automatically send faxes.

To send or manage faxes follow these steps:

1. Click Start, point to All Programs, and point to Accessories.
2. Point to Communications and point to Fax.

Fast User Switching for Multiple Users of a Computer

The Fast User Switching feature allows multiple users to simultaneously share a computer without closing all of their applications first. For example, if you are creating a Microsoft Word document and leave your computer for a short time, Fast User Switching permits another person to use your computer to access another computer account-perhaps to find a customer's account balance-while leaving your Word session open. All of this is done without either of you logging off the computer.

Locale Support Additions and Regional Options Enhancements

A locale is a set of cultural and regional preferences that correspond to a user's language and sublanguage (for example, Canadian French and U.K. English). Compared with Windows 2000 Professional, this feature adds support for the following locales: Galician, Gujarati, Kannada, Kyrgyz, Mongolian (Cyrillic), Punjabi, Divehi, Syriac, and Telugu. The feature also includes enhancements to the Regional and Language Options control panel.

Auto-Configuration for Multiple Network Connectivity

The Auto-Configuration for Multiple Network Connectivity feature provides easy access to network devices and the Internet. It also allows a mobile computer user to seamlessly operate both office and home networks without manually reconfiguring Transmission Control Protocol/Internet Protocol (TCP/IP) settings.

You can use this feature to specify an alternate configuration for TCP/IP if a Dynamic Host Configuration Protocol (DHCP) server is not found. The alternate configuration is useful when a computer is used on multiple networks, one of which does not have a DHCP server and does not use an automatic private Internet Protocol (IP) addressing configuration.

Microsoft Internet Explorer 6.0

Microsoft Internet Explorer 6.0 provides visual refresh and enhanced support for Document Object Model (DOM) Level 1 and Cascading Style Sheets (CSS) Level 1. Internet Explorer 6.0 also provides the following features:

1. Media acquisition enhancements, which include a shortcut menu to make saving images more discoverable and support for My Videos and My Music folders as defaults for those media types.
2. Native support for Macromedia Flash and Macromedia Shockwave Player files.
3. Automatic Image Resize, which allows you to automatically resize an image to fit entirely within the current browser frame. This feature works only when you have directly navigated to an image; it does not resize images embedded within

Hypertext Markup Language (HTML) pages.

Networking has also been enhanced to include changes to cookie handling for improved privacy, and changes to Passport and other authentication dialogs to allow a more integrated password and credential management.

Instant Messaging

Instant Messaging allows users to quickly communicate with one another over the Internet. Internet Explorer 6.0 includes the ability to show MSN Messenger, Outlook Express, and Outlook contacts in a side panel. The Windows Messenger in Windows XP Professional offers multimedia audio, video, and data real-time communication over the Internet. All you need is a .NET passport, which you can create using your Microsoft Hotmail account or using MSN Messenger, and a dial-in connection to the Internet. If you want real-time audio and video, you will need a microphone and a Web cam.

To access Instant Messaging follow these steps:

1. Click Start, point to All Programs, and then click Internet Explorer.
2. Click Online Buddies, and double-click the contact name for the person you want to talk to.

If you are using a Web cam, you will have to click Start for the camera and both you and your friend will need to be using Windows Messenger and have audio/video enabled on your computers.

Internet Connection Firewall (ICF)

Microsoft designed the Internet Connection Firewall (ICF) for use in the home and by small businesses. It provides protection on computers directly connected to the Internet. It is available for LAN or dial-up networking, virtual private networking (VPN), and Point-to-Point Protocol over Ethernet (PPPoE) connections. It also prevents scanning of ports and resources (file and printer shares) from external resources.

Terminal Services: Remote Desktop and Remote Desktop Connection

Windows XP Professional includes two Terminal Services features: Remote Desktop and Remote Desktop Connection. Remote Desktop provides access to a desktop from any Terminal Services client. It also allows you to access the following:

The full set of installed applications, work in progress, and all connectivity usually found on a workstation or server

Sessions on a computer running Windows 2000 Server products that can be used for computer administration or server-based computing

In addition, Remote Desktop enables Remote Console access, allowing the primary screen output to be redirected to a Terminal Server client.

The Remote Desktop Connection feature is the end-user tool for establishing connections to computers running Terminal Services. Corporate employees who work at home, using a line-of-business application that is hosted on a Terminal Server, can use the Remote Access Service (RAS) to dial in and the Remote Desktop Connection to use the application. Remote Desktop Connection has many features that allow optimization for almost any network speed.

To access the Remote Desktop Connection follow these steps:

1. Click Start, and then point to All Programs.
2. Point to Accessories, point to Communications, and then click Remote Desktop Connection. Windows XP Professional displays the Remote Desktop Connection dialog box, as shown in Figure

Figure *The Remote Desktop Connection dialog box*

Understanding Workgroups and Domains

Windows XP Professional supports two secure network environments in which users are able to share common resources, regardless of network size: workgroups and domains.

Workgroups

A Windows XP Professional *workgroup* is a logical grouping of networked computers that share resources, such as files and printers. A workgroup is also called a *peer-to-peer network* because all computers in the workgroup can share resources as equals (peers) without a dedicated server.

Each computer in the workgroup maintains a *local security database*, which is a list of user accounts and resource security information for the computer on which it resides. Therefore, using a local security database decentralizes the administration of user accounts and resource security in a workgroup. Figure 1.10 shows a local security database.

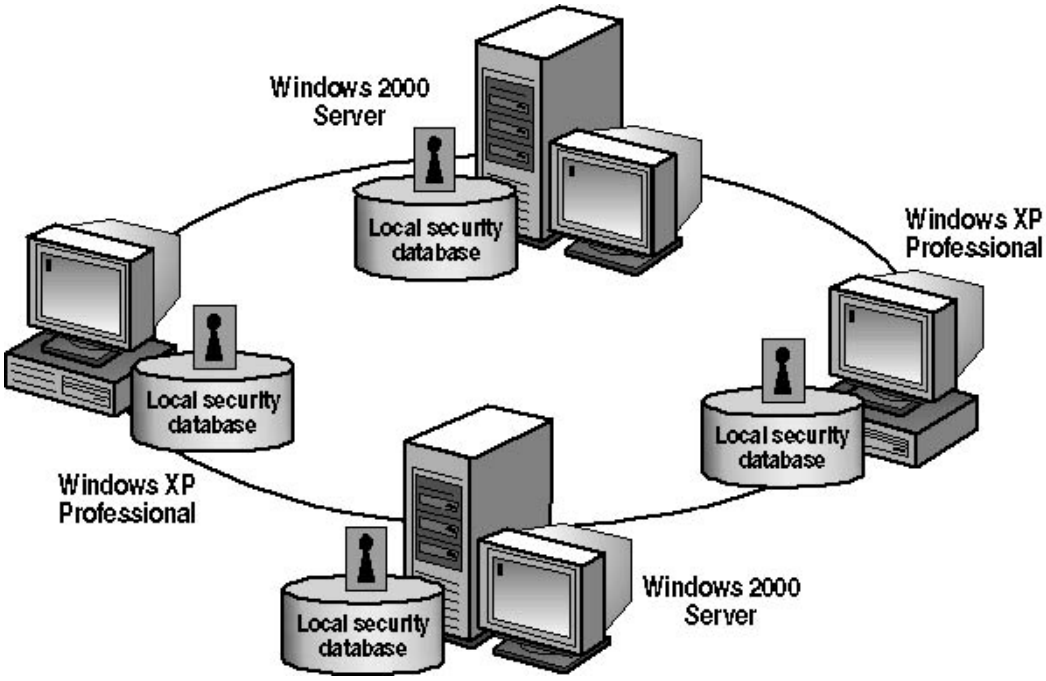


Figure *An example of a Windows XP Professional workgroup*

A workgroup can contain computers running one of the Microsoft Windows NT and Windows 2000 Server products as long as the server is not configured as a domain controller. (Domain controllers are explained later in this lesson.) In a workgroup, a computer running Windows NT or Windows 2000 Server is called a *stand-alone server*.

Because workgroups have decentralized administration and security, the following are true:

1. A user must have a user account on *each* computer to which he or she wants to gain access.
2. Any changes to user accounts, such as changing a user's password or adding a new user account, must be made on each computer in the workgroup. If you forget to add a new user account to one of the computers in your workgroup, the new user will not be able to log on to that computer and will be unable to access resources on it.

A workgroup provides the following advantages:

It does not require inclusion of a domain controller in the configuration to hold centralized security information.

1. It is simple to design and implement. It does not require the extensive planning and administration that a domain requires.
2. It is a convenient networking environment for a limited number of computers in close proximity. However, a workgroup becomes impractical in environments with more than 10 computers.

Domains

A *domain* is a logical grouping of network computers that share a central directory database (see Figure 1.11). A *directory database* contains user accounts and security information for the domain. This database is known as the directory and is the database portion of Active Directory service, the Windows 2000 directory service.

File Systems

After you create the installation partition, Setup prompts you to select the file system with which to format the partition. Like Microsoft Windows NT 4 and Microsoft

Windows 2000 Professional, Windows XP Professional supports the NT file system (NTFS) and file allocation table (FAT). Both Windows 2000 Professional and Windows XP Professional support FAT32. Figure 2.1 summarizes some of the features of these file systems.

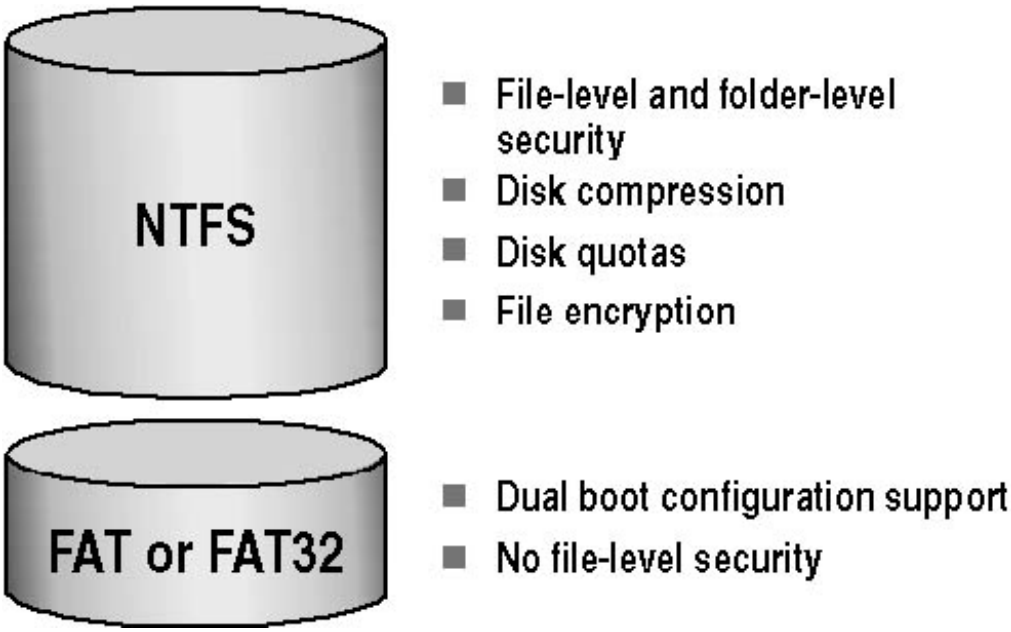


Figure 2.1 *NTFS and FAT/FAT32 file system features*

Use NTFS when the partition on which Windows XP Professional will reside requires any of the following features:

File- and folder-level security. NTFS allows you to control access to files and folders. For additional information, see Chapter 8, "Securing Resources with NTFS Permissions."

Disk compression. NTFS compresses files to store more data on the partition. For additional information, see Chapter 14, "Managing Data Storage."

Disk quotas. NTFS allows you to control disk usage on a per-user basis. For additional information, see Chapter 14, "Managing Data Storage."

Encryption. NTFS allows you to encrypt file data on the physical hard disk, using the Microsoft Encrypting File System (EFS). For additional information, see Chapter 14, "Managing Data Storage."

The version of NTFS in Windows XP Professional supports remote storage, dynamic volumes, and mounting volumes to folders. Windows XP Professional, Windows 2000, and Windows NT are the only operating systems that can access data on a local hard disk formatted with NTFS.

FAT and FAT32

FAT and FAT32 offer compatibility with other operating systems. You must format the system partition with either FAT or FAT32 if you will dual boot Windows XP Professional and another operating system that requires FAT or FAT32.

FAT and FAT32 do not offer many of the features (for example, file-level security) that NTFS supports. Therefore, in most situations, you should format the hard disk with NTFS. The only reason to use FAT or FAT32 is for dual booting with another operating system that does not support NTFS. If you are setting up a computer for dual booting, you need to format only the system partition as FAT or FAT32. For example, if drive C is the system partition, you could format drive C as FAT or FAT32 and format drive D as NTFS.

Converting a FAT or FAT32 Volume to NTFS

Windows XP Professional provides the Convert command for converting a partition to NTFS without reformatting the partition and losing all the information on the partition. To use the Convert command, click Start, click Run, type **cmd** in the Open

text box, and then click OK. This opens a command prompt, which you use to request the Convert command. The following example shows how you might use switches with the Convert command.

Convert *volume* /FS:NTFS [/V] [/CvtArea:filename] [/Nosecurity] [/X]

Table 2.2 lists the switches available in the Convert command and describes their functions.

Table 2.2 *Convert Command Switches*

Switch	Function	Required
Volume	Specifies the drive letter (followed by a colon), volume mount point, or volume name that you want to convert	Yes
/FS:NTFS	Specifies converting the volume to NTFS	Yes
/V	Runs the Convert command in verbose mode	No
/CvtArea:*filename*	Specifies a contiguous file in the root directory to be the placeholder for NTFS system files	No
/NoSecurity	Sets the security settings to make converted files and directories accessible by everyone	No
/X	Forces the volume to dismount first if necessary, and all open handles to the volume are then not valid	No

For help with any command-line program, at the command prompt type the command followed by ***/?*** and then press *Enter*. For example, to receive help on the Convert command, type **Convert /?** and then press *Enter*.

Domain

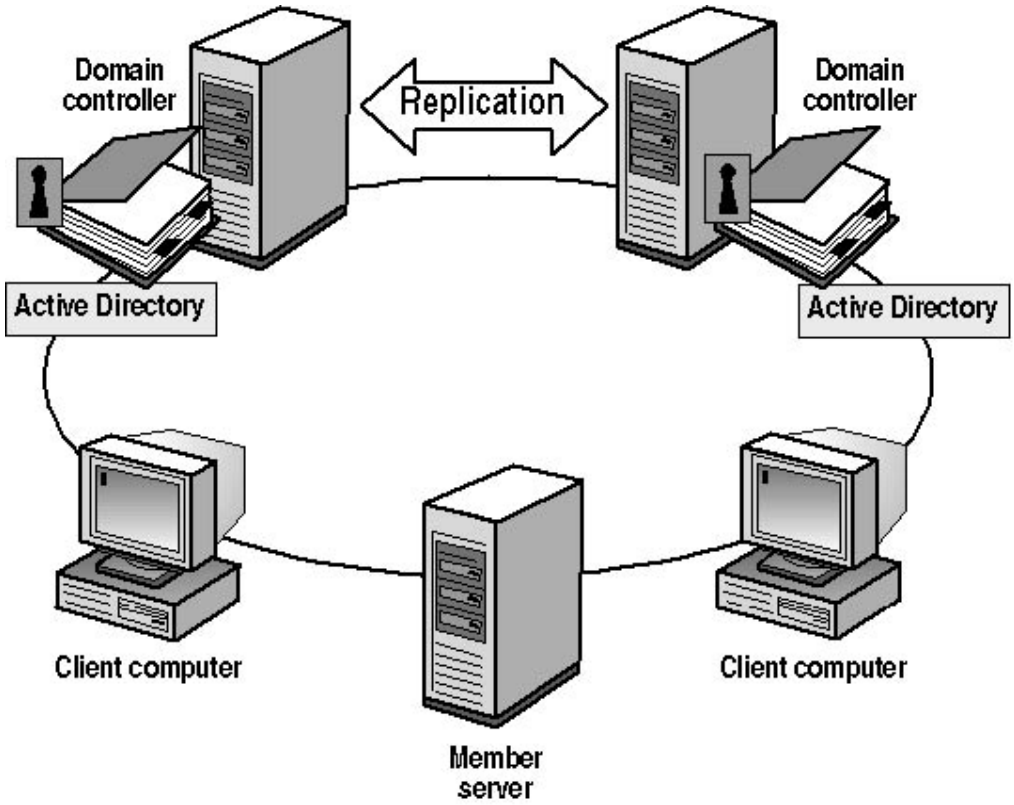


Figure *A Windows 2000 domain*

In a domain, the directory resides on computers that are configured as domain controllers. A *domain controller* is a server that manages all security-related aspects of

user and domain interactions, centralizing security and administration.

You can designate only a computer running one of the Microsoft Windows 2000 Server products as a domain controller. If all computers on the network are running Windows XP Professional, the only type of network available is a workgroup.

A domain does not refer to a single location or specific type of network configuration. The computers in a domain can share physical proximity on a small LAN, or they can be located in different corners of the world. They can communicate over any number of physical connections, including dial-up lines, Integrated Services Digital Network (ISDN) lines, fiber lines, Ethernet lines, token ring connections, frame relay connections, satellite connections, and leased lines.

The benefits of a domain include the following:

- Centralized administration, because all user information is stored centrally.
- A single logon process for users to gain access to network resources (such as file, print, and application resources) for which they have permissions. In other words, you can log on to one computer and use resources on another computer in the network as long as you have appropriate permissions to access the resource.
- Scalability, so that you can create very large networks.

A typical Windows 2000 domain includes the following types of computers:

- **Domain controllers running Windows 2000 Server.** Each domain controller stores and maintains a copy of the directory. In a domain, you create a user account once, which Windows 2000 records in the directory. When a user logs on to a computer in the domain, a domain controller authenticates the user by checking the directory for the user name, password, and logon restrictions. When there are multiple domain controllers in a domain, they periodically replicate their directory information.
- **Member servers running Windows 2000 Server.** A *member server* is a server that is not configured as a domain controller. A member server does not store directory information and cannot authenticate users. Member servers provide shared resources such as shared folders or printers.
- **Client computers running Windows XP Professional, Windows 2000 Professional, or one of the other Microsoft Windows client operating systems.** Client computers run a user's desktop environment and allow the user to gain access to resources in the domain.

Installing Windows XP Professional from a CD-ROM

In this practice, you install Windows XP Professional from a CD-ROM on to a computer that contains no partitions or operating systems. If your computer will not boot from a CD-ROM or if there is already an operating system loaded on your computer, go to Practice 2 to install Windows XP Professional from a CD-ROM without having to boot from the Windows XP Professional installation CD-ROM.

To run the Setup program

1. Insert the Windows XP Professional CD-ROM into the CD-ROM drive and turn on the computer.
2. Some computers will require you to press a key to boot from the CD-ROM drive. If you are prompted to press any key to boot from the CD, press the spacebar.

   Setup displays the Windows Setup screen while it is loading files, and then displays the Windows XP Professional Setup screen.

If you are loading an Evaluation Edition of Windows XP Professional, press *Enter* to continue (or F3 to quit Setup). Setup displays the Welcome To Setup screen.

You can also use Windows XP Professional Setup to repair or recover a damaged Windows XP Professional installation. 2. Read the Welcome To Setup screen and press *Enter* to continue Setup displays the Windows XP Licensing Agreement screen.

3. Read the licensing agreement, and press F8 to agree with the licensing terms.Setup displays another screen, which prompts you to create a partition in which to install Windows XP Professional.

   If you want to use only a portion of the available space, enter the amount of space you want to use and then press E*nter*. You must create a space of at least 2000 MB in size.

4. Select an area of un partitioned space, at least 2000 MB in size, and press C. Setup prompts you to enter a size for the partition.

5. If you want to use all the available space to create the partition, press E*nter*.

   If you already have partitions created, you can also delete partitions at this time. If you have a C partition, you might not be able to delete it because Setup has already loaded some files onto it.

   Setup displays the list of existing partitions for you to select a partition for the installation.

6. Press E*nter* to install Windows XP Professional on the partition you created. Because you are installing into a newly created, unformatted partition, Windows XP Professional Setup prompts you to format the partition.

   If you are planning on dual booting your computer with an operating system that does not support NTFS, your C drive cannot be formatted with NTFS. You might want to install Windows XP Professional in a different drive and format that drive with NTFS.

7. When prompted, format the partition with NTFS. If you format the partition with the FAT file system, Windows XP Professional provides the Convert command, which you can use to convert a partition to NTFS after installation is complete without reformatting the partition and losing all the information contained on the partition.

   Setup formats the hard drive, examines it, and then copies files to the Windows XP Professional installation folders. 8. When Setup prompts you to restart the computer, remove all the disks from the drives, and then press *Enter*.

Ensure that you remove the Windows XP Professional CD-ROM from the CD-ROM drive. If you don't and your computer supports booting from the CD-ROM drive, the computer can attempt to reboot from the CD-ROM. If this happens, remove the CD-ROM and then restart the computer.

The computer restarts. A message box appears, prompting you to insert the Windows XP Professional CD-ROM into your CD-ROM drive.

To run the Setup Wizard

1. Insert the Windows XP Professional CD-ROM into your CD-ROM drive, and then click OK. The Setup Wizard displays a Files Needed dialog box prompting you to verify the path to the Windows XP Professional installation files.

2. Ensure the path to the Windows XP Professional installation files is correct and then click OK. Windows installs the files. This might take several minutes. The Setup Wizard prompts you to customize Windows XP Professional for different regions and languages.

3. Select the appropriate system locale, user locale, and keyboard layout or ensure that they are correct for your language and location, and then click Next. The Setup Wizard displays the Personalize Your Software page, prompting you for your name and organization name. Setup uses your organization name to generate the default computer name. Many applications that you install later will use this information for product registration and document identification.

4. In the Name box, type your name. In the Organization box, type the name of your organization, and then click Next. The Setup Wizard displays the Your Product Key page.

5. Enter your 25-character product key located on the back of the Windows XP Professional CD-ROM case, and then click Next. The Setup Wizard displays the Computer Name And Administrator Password page.

6. Type **Pro1** in the Computer Name box.

   Windows XP Professional displays the computer name in all uppercase letters, no matter how you type it.

   If your computer is on a network, check with the network administrator before assigning a name to your computer. The practice sessions in this training kit refer to Pro1. If you do not name your computer Pro1, you must substitute the name of your computer in each practice.

7. In the Administrator Password box and in the Confirm Password box, type **password**, and then click Next.

8. For the practice sections in this training kit, you will use *password* for the Administrator account. You should always use a complex password for the Administrator account (one that others cannot easily guess). Microsoft recommends mixing uppercase and lowercase letters, numbers, and symbols (for example, Lp6*g9f2).

   The Setup Wizard displays the Modem Dialing Information page.

   If the Setup Wizard does not display the Modem Dialing Information page, it is probably because there is not a modem installed on your computer. Skip to step 12. 8. Ensure that the correct country or region is selected.

9. Type the correct area code or city code.

10. If you dial a number to get an outside line, type the number.

11. Ensure that the correct type of phone system is selected, and then click Next.The Setup Wizard displays the Date And Time Settings page.

12. If necessary, adjust the date and time.

13. If necessary, select the time zone for your location from the Time Zone drop-down list.

14. Ensure that the Automatically Adjust Clock For Daylight Saving Changes check box is selected if you want Windows XP Professional to automatically adjust the time on your computer for daylight savings, and then click Next.

If you have configured your computer for dual booting with another operating system that can also adjust your clock for daylight savings, enable this feature for the operating system you use most frequently so that the daylight savings adjustment will occur only once.

The Setup Wizard installs some networking files and then displays the Networking Settings page.

To install Windows Networking

1. Ensure that Typical Settings is selected, and then click Next. The Setup Wizard displays the Workgroup Or Computer Domain page.

2. Ensure that No, This Computer Is Not On A Network, Or Is On A Network Without A Domain is selected and that the workgroup name is WORKGROUP, and then click Next. The Setup Wizard copies files. This process takes several minutes.

To complete the installation

The Setup Wizard finishes the configuration, copies files, and completes the networking portion of the installation. Then the Setup Wizard installs Start menu items, registers components, saves settings, and removes temporary files. This process takes several minutes.

The computer restarts, and the Setup Wizard displays the Welcome To Microsoft Windows page.

If your computer attempts to reboot from the CD-ROM, remove the CD-ROM and then restart the computer.

1. Click Next to continue .The Setup Wizard displays the Will This Computer Connect To The Internet Directly, Or Through A Network page.
2. If you would like to connect to the Internet at this time, select the appropriate connection method, and then click Next. The Setup Wizard displays the Ready To Activate Windows page.

   At some point you will have to activate Windows XP Professional. However, it is not necessary to activate it while you complete this training kit. 3. Click Yes, Activate Windows Over The Internet Now, and then click Next. The Setup Wizard displays The Ready To Register With Microsoft page.
4. Click Yes, I'd Like To Register With Microsoft Now, and then click Next. The Setup Wizard displays the Collecting Registration Information page.
5. Fill in the appropriate text boxes. The Setup Wizard displays the Ready To Send Information page.
6. Click Next. The Setup Wizard displays the Do You Want To Set Up Internet Access Now page.

   Internet access is not required for this training kit. If you want to connect to the Internet at this time, click Yes Help Me Connect To The Internet, click Next and follow the instructions on your screen.
7. Click No, Not At This Time, and then click Next. The Setup Wizard displays the Who Will Use This Computer page. Your name should already be entered.
8. Type **Fred** for the second user, and then click Next. The Setup Wizard displays the Thank You page.
9. Read the page and then click Finish.
10. To log on, select Fred (or the account name created for you during setup).You have completed your installation of Windows XP Professional and logged on as an administrator.

The Windows XP Professional Boot Process

Files Used in the Boot Process

A Windows XP Professional Intel-based boot sequence requires a number of files. A list of these files, their appropriate locations and the stages of the boot process associated with each file are listed in Table below

Note: Systemroot represents the path to your Windows XP Professional installation folder, which by default is C:\Windows

TABLE below shows files Used in the Windows XP Professional Boot Process

File	Location
Ntldr	**System partition root (C:\ )**
Boot.ini	**System partition root**
Bootsect.dos	**System partition root**
Ntdetect.com	**System partition root**
Ntbootdd.sys	**System partition root**
Ntoskrnl.exe	***systemroot*\System32**
Hal.dll	*systemroot*\System32

Note: The string systemroot (typed as %systemroot%) represents the folder in the boot partition that contains the Windows XP Professional system files.

Preboot Sequence

During startup, a Windows XP Professional-based computer initializes the boot portion of the hard disk and the preboot sequence begins. This sequence consists of following steps:

1] The computer runs power-on self test (POST) process to determine the amount of physical memory and the hardware components are present.

2] If the computer has a Plug and Play (BIOS), enumeration and configuration of hardware devices occurs.

3] The computer BIOS locates the boot device and loads and runs the master boot record (MBR).

Note: Windows XP Professional modifies the boot sector during installation so that Ntldr loads during system startup. Therefore you should disable the Boot Sector Virus Protection in your BIOS Setup.

Boot Sequence

After the computer loads Ntldr into memory, the boot sequence gathers information about hardware and drivers in preparation for the Windows XP Professional load phases. The boot sequence uses the following files: Ntldr, Boot.ini, Bootsect.dos (optional), Ntdetect.com, and Ntoskrnl.exe.

The boot sequence also has five phases:

- **Initial Boot Loader Phase :** During the initial boot loader phase, Ntldr switches the microprocessor from real mode to 32-bit flat memory mode, which Ntldr requires. Then, Ntldr starts the appropriate the minifile system drivers. The minifile system drivers are built into Ntldr so that Ntldr can find and load Windows XP Professional from partitions formatted with either the FAT or NTFS file system.
- **Operating System Selection Phase:** During the boot sequence, Ntldr reads the Boot.ini file. If multiple operating systems are supported on the computer in the Boot.ini file, then the Please Select The Operating System To Start screen, which you can use to select the operating system that should be loaded within a specified time before the default operating system. If no Boot.ini file is present, Ntldr attempts to load Windows XP Professional from the Winnt folder on the first partition of the first disk, typically C:\Windows

Hardware Detection Phase: On Intel-based computers, Ntdetect.com and Ntoskrnl.exe perform hardware detection. Ntdetect.com executes if Windows XP Professional should be loads. Ntdetect.com collects a list of installed hardware components and returns this list to Ntldr for later inclusion in the registry under the HKEY_LOCAL_MACHINE\HARDWARE key.

- **Configuration Selection Phase:** After Ntldr starts loading Windows XP Professional and collects hardware information, the operating system loader process displays the Hardware Profile/Configuration Recovery Menu screen, which contains a list of the hardware profiles that have been created on the computer, if more that one hard profile exists on the computer. The first hardware profile is highlighted. You can press the Down arrow key to select another profile. You can also press L to invoke the Last Known Good Configuration option.
- **Windows XP Professional Logon Phase:** The Windows XP Professional boot sequence is complete once the user has successfully logged on at the computer.

Kernel Load

After the configuration selection, Ntoskrnl.exe, the Windows XP kernel loads and initializes. Ntoskrnl.exe also loads and initializes device drivers and loads services. If you press Enter when the Hardware Profile/Configuration Recovery Menu screen displays, or if Ntldr makes the selection automatically, the computer enters the kernel load phase. The screen clears and a series of white rectangles appears across the bottom of the screen. During the kernel load phase, Ntldr:

- Loads Ntoskrnl.exe but does not initialize it.
- Loads the hardware abstraction layer file (Hal.dll).
- Loads the HKEY_LOCAL_MACHINE\SYSTEM registry key.
- Selects the control set required to initialize the computer.
- Loads device drivers with a value of 0x0 for the Start entry. These are typically low-level hardware device drivers, such as those for a hard disk.

When the kernel load phase is complete, the kernel initializes and takes control from Ntldr. The system displays a graphical screen with a status bar that indicates load status. During the kernel initialization stage four tasks are performed:

- The Hardware key is created.
- The Clone control set is created.
- Device drivers are loaded and initialized.
- Services are started.

Logon

The logon process begins at the end of the kernel initialization phase, when the Win32 subsystem automatically starts Winlogon.exe, which starts Local Security Authority (Lsass.exe) and displays the Logon dialog box. This allows you to log on while Windows XP initializes the network device drivers.

Note: Windows XP startup is not considered successful until a user logs on at the computer. After a logon, the system automatically copies the Clone control set to the Last Known Good control set making the current control set the Last Known Good Configuration.

Check Your Progress 10.2

State True or False

1] Windows XP is a Network operating system.

2] Windows XP Professional can take part in Domain Networks.

3] NTFS 5 file system supports user quota and disk quota.

4] You can convert FAT or FAT32 file system to NTFS file system without

Match the followings

1] Windows XP operating system	1] Peer to Peer Network
2] FAT32 file system	2] Desktop Operating System
3] Workgroup	3] No File Level security
4] NTFS	4] c:\windows
5] System root	5] Disk Compression

10.4 SHARING FOLDERS AND PRINTERS

If you set up a Microsoft or Novell network client, you can share your documents-and any printers attached to your computer-with other people on the network. To use file and print sharing, you must first choose which of two types of access you want to give other users.

- Share level control is default access setting. It lets you require a password for each shared resource.
- User-level control lets you specify who has access to each shared resource, but it doesn't let you require a password.

TO CHECK FORM SHARE-LEVEL CONTROL TO USER-LEVEL-CONTROL

1. Click Start, point to settings, click control panel, and double click network.
2. Click the access control tab, and then click User-level access control.
3. In obtained list of users and group from type the name of the domain or server you want to use, and then click ok.
4. You may be prompted to supply additional information about the domain or server you specified.
5. Restart your computer.

To set-up file-and print-sharing services

1. Click Start, point to setting click control panel, and double click network.
2. In the network dialog box, click file and print sharing.
3. Select the check boxes for the sharing options you want, click ok twice

A message prompts you to insert your Windows 98 CD or setup disk so that File and Print sharing can be installed. Then restart your computer.

10.5 TO SHARE A FOLDER WITH SHARE LEVEL ACCESS CONTROL

1. In MY Computer, right click the folder you want to share, and then dick sharing.
2. In the properties dialog box, dick the sharing tab, and then click Shred as
3. In the share name, type a name for the folder. In comment, you can type a brief comment or description of the folder.
4. In access type, click Read only, Full, or Depends On password. Regardless of which type of access you select. You have the option of adding a password.
5. Type a password if you want to use of the and then click ok.

The folder or printer icon changes to a folder or a printer with a hand, including that the item is now shared.

You can use this procedure to share an entire disk drive. Instead of selecting a folder, select a drive icon.

To Share a Folder with User -Level Access Control

1 . In My Computer, right click the folder you want to share, and then click sharing.

2. On the Sharing tab, click shared as
3. In share name, type a for the folder. In comment, you can type a brief comment or a description of the folder.
4. Click add
5. In the Add Users dialog-box, click the name (s) of the persons to whom you want to grant permissions.
6. Click the type of access permissions you want to give the selected users Read only, Full access or Custom
7. Click ok.

To Share a Printer with Share-Level Access Control

1 . In my computer, double click the printer folder

2. Right click the printer you want to share, and then click sharing
3. On the sharing tab, dick shared as
4. In share name, type a name for the printed. I*n* comment you can type brief description, and in password you can type a password that a user must type to use the printer
5. Click ok. If you type the password, retype the password to verify it. Click ok.

To Share a Printer with User-Level Access Control

In My Computer, double click the printer folder.

2. Right click the printer you wan to share, and then click sharing.

3. On the sharing tab, click shared as.
4. In share name, type a name for printer. In comment you can type brief component description of the printer
5. Clicks add.
6. In the add users dialog box, click the names of the people to whom you want to grant permissions.
7. Click full access.

10.6 SUMMARY

An operating system is a part of system software that is loaded into computer on boot up that is responsible for running other applications and provide interfaces to interact with other programs that uses system hardware.

Multitasking is the capability of operating system to handle more than one task of a time.

Two types of Multitasking.

i) Co-operative Multitasking

ii) Preemptive Multitasking.

Windows XP operating system is either 32 bit or 64 bit operating system that run in two different modes which are kernel & user, Windows XP supports three file systems.

i) File Allocation table (Fat16)

ii) FAT 32

iii) New Technology file system (NTFS)

Microsoft designed the internet connection firewall (ICF) for use in the home and by small businesses. It provides protection on computers directly connected to internet, A Windows XP professional supports two secure network environments in which users are able to share common resources, regardless of network size Workgroup and domains.

A domain is a logical grouping of network computers that share a central directory database.

Source : *http://etutorials.org*

10.7 CHECK YOUR PROGRESS – ANSWERS

10.1
Fill in the blanks
1] 32 bit or 64 bit
2] Kernel and User
3] 2 CPUs.
4] 4GB
5] Home

10.2
1] False
2] True
3] True
4] True
5] False

Match the followings
1] – 2]
2] –3]
3] –1]
4] --5]
5] –4] .

10.8 QUESTIONS FOR SELF – STUDY

1) What is operating system?
2) Write a short note on Multitasking.
3) What are the features of Desktop Operating System.
4) What are the features of Windows XP?
5) What are the types of File System?
6) Write a short Note on
   a) Instant Messaging
   b) Internet Connection Firewall
7) What is FAT & FAT 32?
8) What is Boot sequence?

10.9 SUGGESTED READINGS

1. Computer Networks : Andrew Tanenbaum
2. Computer Networks : A Top Down Approach by Behrouz forouzan mosharraf

❁❁❁

NOTES

Chapter 11

Wireless Networks

11.0 OBJECTIVES

After studying this chapter you will be able to-

- ✓ Explain the working of Wireless Networking.
- ✓ State Wireless standards.
- ✓ Discuss advantages and disadvantages of wireless networking.

11.1 INTRODUCTION

Wi-Fi is a brand originally licensed by the Wi-Fi alliance to describe the underlying technology of wireless Local Area Networks (WLAN) based on IEEE 802.11 specifications. Wi-Fi was intended to be used for mobile computing devices, such as Laptops in LANs, but is now often used for increasingly more applications including Internet Access, gaming, and basic connectivity of consumer electronics such as televisions and DVD players.

A person with a Wi-Fi device such as computer, telephone or personal digital assistant (PDA) can connect to the internet when in proximity of an access point. The region covered by one or several access points is called a hot spot. Hot spots can be range from a single room to many square miles of overlapping hot spots.

Wireless Networks uses radio waves as its carrier. (RF 2.4 GHz to 5 GHz). Wi-Fi stands for Wireless Fidelity.

11.2 WORKING OF WIRELESS NETWORKS

The typical Wi-Fi setup contains one or more Access points (APs) and one or more clients. A AP broadcasts its SSID (Service Set Identifier, Network Name) via packets that called beacons, which are broadcasted every 100 ms. The beacons are transmitted at 1 Mb/s and are relatively short and therefore are not of influence on performance. Since 1Mb/s is the lowest rate of Wi-Fi it assures that the client who receives the beacon can communicate at at least 1Mb/s . Based on the settings (e.g. the SSID) , the client may decide whether to connect to an AP. Also the firmware running on the client Wi-Fi is of influence. Say two APs of the same SSID are in the

range of the client, the firmware may decide based on signal strength to which of two APs it will connect.

Wi-Fi uses spectrum near 2.4 GHz, which is a standardized and unlicensed by international agreement.

11.3 EXAMPLES OF WI-FI DEVICES

Wireless Access Point (WAP)

A wireless access point connects a group of wireless stations to adjacent wired local area network (LAN). An access point is similar to an Ethernet Hub, but instead of relaying on LAN data only to other LAN stations, an access point can relay wireless data to all other compatible wireless devices as well as LAN stations connected by wires.

Wireless Routers

A wireless router connects a group of Wi-Fi enabled devices (i.e. PDAs, laptops etc) to adjacent wired network (such as cable modem or DSL modem). A wireless access router is a wireless access point combined with an Ethernet Hub. A wireless router forwards between your wireless subnet and any other subnet.

Wireless Ethernet Bridge

A wireless Ethernet Bridge connect two separate networks.

Wi-Fi supported operating systems:-

1] Microsoft Windows XP, Vista and Windows 7 have a good support for wireless.

2] Mac Operating system has good Wi-Fi support and operating system includes native support for Apple “AirPort” Wi-Fi cards.

3] Linux has excellent support for most of wireless cards.

11.1 Check Your Progress

Fill in the blanks

A] Wi-Fi stands for ……..

B] Wi-Fi users ……..as its carrier.

C] A ……..connects a group of wireless stations to adjacent wired local area network (LAN).

D] A ……..connect two separate networks.

Wireless Capabilities :-

1] It provides temporary connections to and existing cable (Wired) networks.

2] Provides backup (redundant) to an existing wired networks.

3] Extend the networks beyond the limits of copper or even fiber optic cables.

Usage of Wireless Networks:-

1] Busy areas such as lobbies, and reception areas.

2] For people who are constantly on move such as doctors in hospitals, in isolated areas.

3] Buildings or departments where physical settings changes frequently.

3] Structures such as historical buildings where cabling would be difficult.

11.4 WIRELESS STANDARDS

IEEE 802.11 is a set of standards carrying out Wireless Local Area Network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802).

General description

A Compaq 802.11b PCI card

The 802.11 family includes over-the-air modulation techniques that use the same basic protocol. The most popular are those defined by the 802.11b and 802.11g protocols, which are amendments to the original standard. 802.11-1997 was the first wireless networking standard, but 802.11b was the first widely accepted one, followed by 802.11g and 802.11n. Security was originally purposefully weak due to export requirements of some governments and was later enhanced via the 802.11i amendment after governmental and legislative changes. 802.11n is a new multi-streaming modulation technique. Other standards in the family (c–f, h, j) are service amendments and extensions or corrections to the previous specifications.

802.11b and 802.11g use the 2.4 GHz ISM band, operating in the United States under Part 15 of the US Federal Communications Commission Rules and Regulations. Because of this choice of frequency band, 802.11b and g equipment may occasionally suffer interface from microwave ovens, cordless telephones and Bluetooth devices. Both 802.11 and Bluetooth control their interference and susceptibility to interference by using spread spectrum modulation. Bluetooth uses a frequency hopping spread spectrum signaling method(FHSS), while 802.11b and 802.11g use the direct sequence spread spectrum signaling (DSSS) and orthogonal frequency division multiplexing (OFDM) methods, respectively. 802.11a uses the 5GHz U-NII band, which, for much of the world, offers at least 19 non-overlapping channels rather than the 3 offered in the 2.4 GHz ISM frequency band. Better or worse performance with higher or lower frequencies (channels) may be realized, depending on the environment.

The used segment of the radio frequency spectrum varies between countries. In the US, 802.11a and 802.11g devices may be operated without a license, as allowed in Part 15 of the FCC Rules and Regulations. Frequencies used by channels one through six (802.11b) fall within the 2.4 GHz amateur radio band. Licensed amateur radio operators may operate 802.11b/g devices under part 97 of the FCC Rules and Regulations, allowing increased power output but not commercial content or encryption.

The original version of the standard IEEE 802.11 was released in 1997 and clarified in 1999, but is today obsolete. It specified two net bit rates of 1 or 2 megabits per seconds (Mbit/s), plus forward error corrections code. It specified three alternative physical layer technologies: diffuse infrared operating at 1 Mbit/s; frequency hopping spread spectrum operating at 1 Mbit/s or 2 Mbit/s; and direct sequence spread

spectrum operating at 1 Mbit/s or 2 Mbit/s. The latter two radio technologies used microwave transmission over the Industrial Scientific Medical Frequency Band at 2.4 GHz. Some earlier WLAN technologies used lower frequencies, such as the U.S. 900 MHz ISM band.

Legacy 802.11 with direct-sequence spread spectrum was rapidly supplanted and popularized by 802.11b.

802.11a

Release date	Op. Frequency	Throughput	Net Bit Rare (max.)	Gross Bit Rate (max.)	Max Indoor Range	Max Outdoor Range
October 1999	**5 GHz**	**20 Mbit/s**	**54 Mbit/s**	**72 Mbit/s**	**~75 ft/25 meters**	**~150 ft/50 meters**

The 802.11a standard uses the same data link layer protocol and frame format as the original standard, but an OFDM based air interface (physical layer). It operates in the 5 GHz band with a maximum net data rate of 54 Mbit/s, plus error correction code, which yields realistic net achievable throughput in the mid-20 Mbit/s . Since the 2.4 GHz band is heavily used to the point of being crowded, using the relatively un-used 5 GHz band gives 802.11a a significant advantage. However, this high carrier frequency also brings a disadvantage: the effective overall range of 802.11a is less than that of 802.11b/g. In theory, 802.11a signals are absorbed more readily by walls and other solid objects in their path due to their smaller wavelength and, as a result, cannot penetrate as far as those of 802.11b. In practice, 802.11b typically has a higher range at low speeds (802.11b will reduce speed to 5 Mbit/s or even 1 Mbit/s at low signal strengths). However, at higher speeds, 802.11a often has the same or greater range due to less interference.

802.11b

Release date	Op. Frequency	Throughput (typ.)	Net Bit Rate (max.)	Gross Bit Rate (max.)	Max Indoor Range	Max Outdoor Range
October 1999	**2.4 GHz**	**~5 Mbit/s**	**11 Mbit/s**	**11 Mbit/s**	**~150 feet/45 meters**	**~300 feet/90 meters**

802.11b has a maximum raw data rate of 11 Mbit/s and uses the same media access method defined in the original standard. 802.11b products appeared on the market in early 2000, since 802.11b is a direct extension of the modulation technique defined in the original standard. The dramatic increase in throughput of 802.11b (compared to the original standard) along with simultaneous substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.

802.11b devices suffer interference from other products operating in the 2.4 GHz band. Devices operating in the 2.4 GHz range include: microwave ovens, Bluetooth devices, baby monitors and cordless telephones.

802.11g

Release date	Op. Frequency	Throughput (typ.)	Net Bit Rate (max.)	Gross Bit Rate (max.)	Max Indoor Range	Max Outdoor Range
June 2003	**2.4 GHz**	**~22 Mbit/s**	**54 Mbit/s**	**128 Mbit/s**	**~150 feet/45 meters**	**~300 feet/90 meters**

In June 2003, a third modulation standard was ratified: 802.11g. This works in the 2.4 GHz band (like 802.11b), but uses the same OFDM based transmission scheme as 802.11a. It operates at a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 22 Mbit/s average throughput. 802.11g hardware is fully backwards compatible with 802.11b hardware and therefore

is encumbered with legacy issues that reduce throughput when compared to 802.11a by ~21%.

The then-proposed 802.11g standard was rapidly adopted by consumers starting in January 2003, well before ratification, due to the desire for higher data rates as well as to reductions in manufacturing costs. By summer 2003, most dual-band 802.11a/b products became dual-band/tri-mode, supporting a and b/g in a single mobile adapter card or access point. Details of making b and g work well together occupied much of the lingering technical process; in an 802.11g network, however, activity of an 802.11b participant will reduce the data rate of the overall 802.11g network.

Like 802.11b, 802.11g devices suffer interference from other products operating in the 2.4 GHz band.

In 2003, task group TG ma was authorized to "roll up" many of the amendments to the 1999 version of the 802.11 standard. REV ma or 802.11ma, as it was called, created a single document that merged 8 amendments (802.11a,b,d,e,g,h,i,j) with the base standard. Upon approval on March 8, 2007, 802.11REVma was renamed to the current base standard **IEEE 802.11-2007**.

802.11n

802.11n is a recent amendment which improves upon the previous 802.11 standards by adding multiple –input multiple –output (MIMO) and many other newer features. The IEEE has approved the amendment and it was published in October 2009. Prior to the final ratification, enterprises were already migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11n proposal.

Release date	Op. Frequency	Throughput (typ.)	Net Bit Rate (max.)	Gross Bit Rate (max.)	Max Indoor Range	Max Outdoor Range
September 11, 2009	**5 GHz and/or 2.4 GHz**	**50–144 Mbit/s**	**600 Mbit/s**	**450 Mbit/s**	**~229 feet/70 meters**	**~820 feet/250 meters**

Modes of Operations

Peer to Peer or Ad-Hoc Mode

This is a method for wireless devices to directly communicate with each other. Operating in ad-hoc mode allows wireless devices within range of each other to discover and communicate in peer to peer fashion without involving central access points.

This is typically used by two PCs to connect to one another so that one can share the other's internet connection for example as well as for wireless mesh networks.

Infrastructure Mode (Access point /Client)

The most common is to have access points wired to Internet, and having wireless clients (typically Laptops) accessing Internet through the access point. This is also called as Infrastructure Mode.

11.5 ADVANTAGES AND DISADVANTAGES OF WIRELESS NETWORKS

Advantages of Wireless Networks

1] Allows LANs to be deployed without cabling, potentially reducing costs of network deployment and expansion. Spaces where cables cannot be run, such as outdoor areas and historical buildings, can host wireless networks.

2] Wi-Fi silicon pricing continues to come down, making Wi-Fi a very economical networking option.

3] Wi-Fi products are widely available in the market. Different brands of access points and client network interfaces are interoperable at the basic level of service.

4] Wi-Fi networks support roaming, in which a mobile client station such as a laptop can move from one access point to another as the user moves around in the building areas.

Disadvantages of Wireless Networks

1] Power consumption is fairly high, making battery life and heat a concern.

3] The most common wireless encryption standard, Wired Equivalent Privacy or WEP has been shown to be breakable even when correctly configured.

3] Wi-Fi networks have limited range. A typical Wi-Fi home router using 802.11b or 802.11g standard with a stock antenna might have a range of 45 Meters (Indoor) and 90 Meters (outdoor).

4] Wi-Fi networks can be monitored and used to read and copy data (including personal information) transmitted over the network when encryption is not enabled.

5] The frequency which 802.11b and 802.11g operates is 2.4GHz which can lead to interference with cordless phones in the super high frequency range.

11.2 Check your progress

Fill In the blanks

1] …….. is IEEE standard for Wireless Networks.

2] 802.11a wireless standard supports data transfer speed up to ……...

3] 802.11b wireless standard supports data transfer speed up to ……...

4] 802.11g wireless standard supports data transfer speed up to ……...

5] 802.11n wireless standard supports data transfer speed up to ……...

6] There are two modes of operation for wireless networks …….. and ……...

7] WEP stands for ……..……...

8] WPA stands for ……..……...

State True or false

1] Wireless networks are secured networks……...

2] Wireless Access points are required in Infrastructure Mode. ……

3] Power consumption of wireless devices is very less. ……...

4] Wi-Fi networks has unlimited network range. ……..

5] Wireless networks are easy to configure**.** ……...

11.6 WIRELESS SECURITY

WEP (Wired Equivalent Privacy)

Short for ***W****ired* ***E****quivalent* ***P****rivacy*, a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. LANs are inherently more secure than WLANs because LANs are somewhat protected by the physical of their structure,

having some or all part of the network inside a building that can be protected from unauthorized access. WLANs, which are over radio waves, do not have the same physical structure and therefore are more vulnerable to tampering. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security.

Wi-Fi Protected Access

Wi-Fi Protected Access (**WPA** and **WPA2**) a certification program created by the Wi-Fi Alliance to indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks. This protocol was created in response to several serious weaknesses researchers had found in the previous system, WEP (Wired Equivalent Privacy)

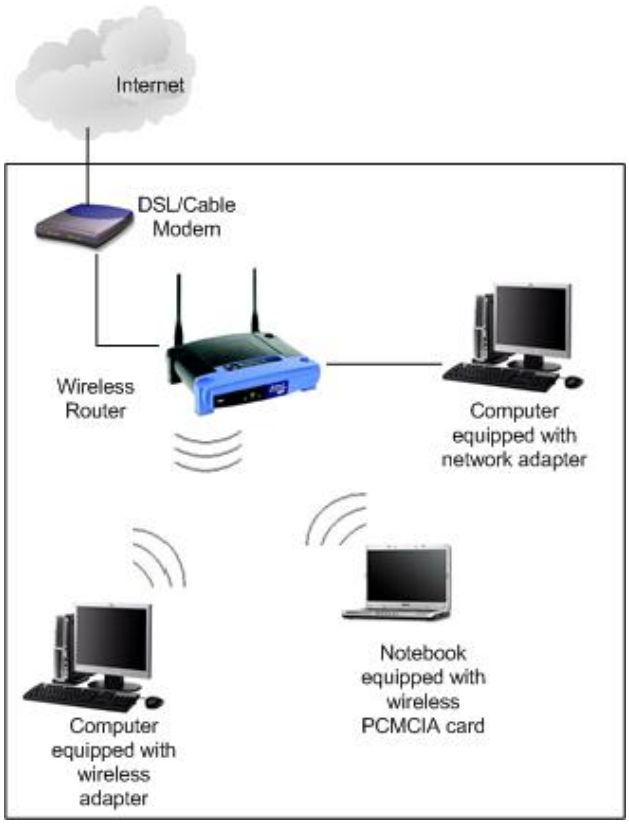
The WPA protocol implements the majority of the IEEE802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. Specifically, the Temporal Key Integrity Protocol (TKIP), was brought into WPA. TKIP could be implemented on pre-WPA Wireless Network Interface Cards that began shipping as far back as 1999 through firmware upgrades. Because the changes required fewer modifications on the client than on the Wireless Access Point, most pre-2003 APs could not be upgraded to support WPA with TKIP. Researchers have since discovered a flaw in TKIP that relied on older weaknesses to retrieve the key stream from short packets to use for re-injection and spoofing

The later WPA2 certification mark indicates compliance with an advanced protocol that implements the full standard. This advanced protocol will not work with some older network cards. Products that have successfully completed testing by the Wi-Fi Alliance for compliance with the protocol can bear the WPA certification mark.

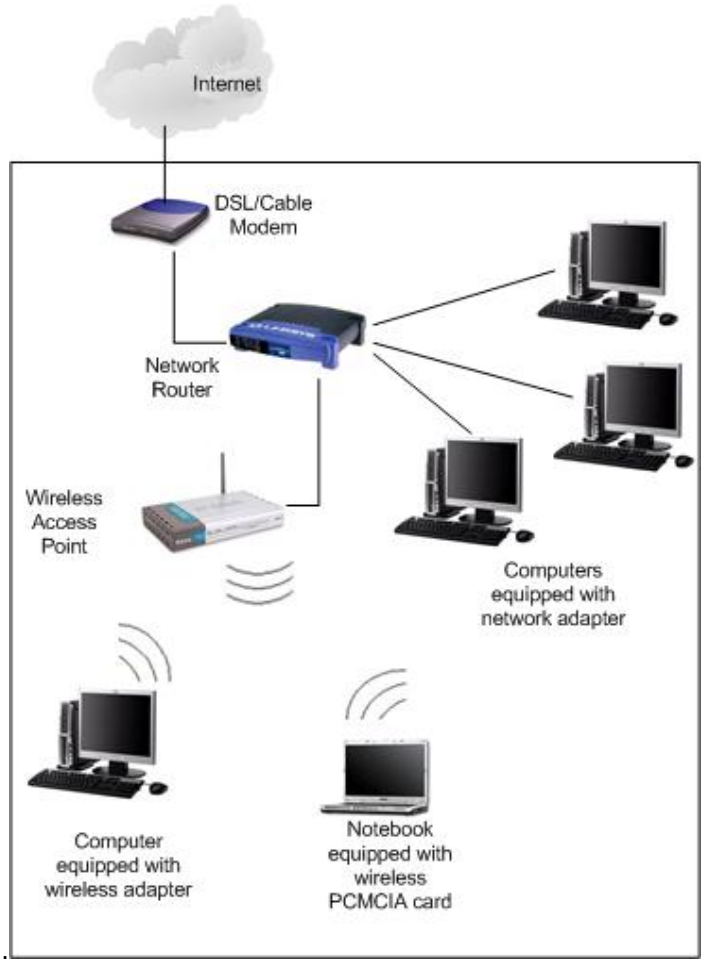
11.7 EXAMPLES OF WIRELESS NETWORKS

Wireless Network is a network setup by using radio signal frequency to communicate among computers and other network devices. Sometimes it is also referred to as Wi-Fi network or WLAN. This network is now getting popular due to easy set up feature and no cabling involved. You can connect computers anywhere in your home without need for wires.

Here is a simple explanation of how it works. Let say you have two computers each equipped with wireless adapter and you have set up wireless router. When the computer send out the data, the binary data will be encoded to RF (Radio Frequency) and transmitted via wireless router. The receiving computer will then decode the signal back to binary data. It doesn't matter that you are using broadband cable/DSL modem to access internet, both ways will work with wireless network. The area covered by wireless devices is called as hotspot. The two main components are wireless router or access point and wireless clients. If you have not setup any wired network, then just get a wireless router and attach it to cable/DSL modem. You then setup wireless client by adding a wireless card to each computer and form a simple wireless network. You can also cable connect computer (Wired Computer) directly to router if there are switch ports available.



If you already have wired Ethernet Network at home you can attach wireless access point to existing network router and have wireless access at home



Wireless router or access points should be installed in a way that maximizes coverage as well as throughput. The coverage provided is generally referred to as the coverage cell. Large areas usually requires more than one access point in order to

have adequate coverage. You can also add access point to existing wireless router to improve the coverage.

Wireless Operating Mode

The IEEE 802.11 standards is used to connect computers with wireless network adapters, also known as wireless clients, to an existing wired network with the help from wireless router or access point. The two examples specified above operates in this mode. This is known as infrastructure mode.

Ad hoc mode is used to connect wireless clients directly together (Peers) without the need for wireless router or access point. An ad hoc network consists of up to 9 wireless clients, which send their data directly to each other.

11.8 SUMMARY

Wi-Fi underlying technology of wireless Local Area Network (WLAN) based on LEEE 802.11 specification. The typical Wi-Fi set up contains one or more Access Points (AP) and one or more clients. Wi-Fi uses spectrum near 2.4 GHz which is a standardized and unlicensed by international agreement. Examples of Wi-Fi devices are WAP, Wireless Routers. Wireless Ethernet Bridge.

IEEE 802.11 is a set of Wireless standard carrying out WLAN communication. There are two types of Mode of operations

i)Peer to peer or Ad-Hoc Mode.

ii) Infrastructure Mode

Wifi silicon pricing continues to come down, making Wi-Fi a very economical networking option. The disadvantage of wireless Network is about power consumption. The power consumption is very high, making battery life and heat a concern.

Wired Equivalent Privacy (WEP) is a security protocol for WLAN. WEP is designed to provide the same level of security as that of wired LAN LAN's are inherently more secure than WLAN.

Source : *http://centralupload.com(Link)*

11.9 CHECK YOUR PROGRESS – ANSWERS

11.1

Fill in the blanks

A] Wireless Fidelity. B] Radio waves.
C] Wireless Access Point D] Wireless Bridge

11.2

1] 802.11 2] 54Mbps 3] 11Mbps 4] 54Mbps
5] 600Mbps
6] Peer to Peer Mode and Infrastructure Mode
7] Wired Equivalent Privacy 8] WPA

State True or false

1] False 2] True 3] False 4] False 5] True

11.10 QUESTIONS FOR SELF–STUDY

1) Write a short Note on Wireless Network
2) What are the examples of Wi-Fi devices?
3) What are the Wireless standards?
4) What are the advantages & disadvantages of Wireless Network?
5) Write a short Note on wireless Security.

11.11 SUGGESTED READINGS

1. Computer Networks : Andrew Tanenbaum
2. Computer Networks : A Top Down Approach by Behrouz forouzan mosharraf
3. Networking Essentials : Emmett Dulaney

❁❁❁

NOTES