CS-13 Network Technology and Administration

BCA Semester-3

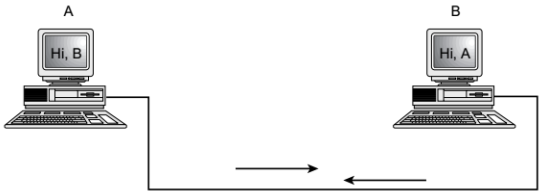
Unit-1

Basics of Network, Network Models and LAN Sharing

1.1 Network concepts

Modern world scenario is ever changing. Data Communication and network have changed the way business and other daily affair works. Now, they highly rely on computer networks and internetwork. A set of devices often mentioned as nodes connected by media link is called a Network. A node can be a device which is capable of sending or receiving data generated by other nodes on the network like a computer, printer etc. These links connecting the devices are called Communication channels.

1.1.1 What is network?



Networking is the concept of sharing resources and services. A network of computers is a group of interconnected systems sharing resources and interacting using a shared communications link (see Figure). A network, therefore, is a set of interconnected systems with something to share. The shared resource can be data, a printer, a fax modem, or a service such as a database or an email system. The individual systems must be connected through a pathway (called the transmission medium) that is used to transmit the resource or service between the computers. All systems on the pathway must follow a set of common communication rules for data to arrive at its intended destination and for the sending and receiving systems to understand each other. The rules governing computer communication are called protocols. In short all networks must have the following:

- A resource to share (resource)
- A pathway to transfer data (transmission medium)
- A set of rules governing how to communicate (protocols)

1.1.2 Use of network

Had it not been of high importance, nobody would have bothered connecting computers over a network. Let's start exploring the uses of Computer Networks with some traditional use cases at companies and for individuals and then move on to the recent developments in the area of mobile users and home networking.

Business Applications: Following are some business applications of computer networks

1. Resource Sharing:
2. Server-Client model:
3. Communication Medium:
4. E-Commerce:

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

1. Access to remote information
2. Person-to-person communication
3. Interactive entertainment
4. Electronic commerce

Mobile Users: Mobile computers, such as notebook computers and Mobile phones, is one of the fastest-growing segment of the entire computer industry. Although wireless networking and mobile computing are often related, they are not identical.

1.2 Network model

Networks generally fall into one of two broad network categories:Peer-to-peer networks and Client/server networks. It is important to remember that one type of networking configuration is not necessarily better than another. Each type of networkingmodel has its own strengths and weaknesses.

1.2.1 Peer- to- Peer

A peer-to-peer network consists of a group of PCs that operate asequals. Each PC is called a peer. The peers share resources (such asfiles and printers) just like in a server-based network, although nospecialized

or dedicated server machines exist. In short, each PC can act as a client or a server. No one machine is set up with a higher powered set of devices, nor is any one PC set up simply to provideone service (such as storing files). Small networks—usually with fewer than 10 machines—can work well in this configuration. Inlarger networks, companies usually move to a server-based network because many clients requesting to use a shared resource can put too much strain on one client's PC. Examples of peer-to-peer networksinclude Windows for Workgroups, Windows XP, and Windows 7/8.Peer-to-peer networks can work well for small workgroups.

1.2.2 Client/Server

A client/server network consists of a group of user-oriented PCs(called clients) that issue requests to a server. The client PC is responsible for issuing requests for services to be rendered. The server'sfunction on the network is to service these requests. Servers generallyare higher-performance systems that are optimized to provide network services to other PCs. The server machine often has a fasterCPU, more memory, and more disk space than a typical clientmachine.

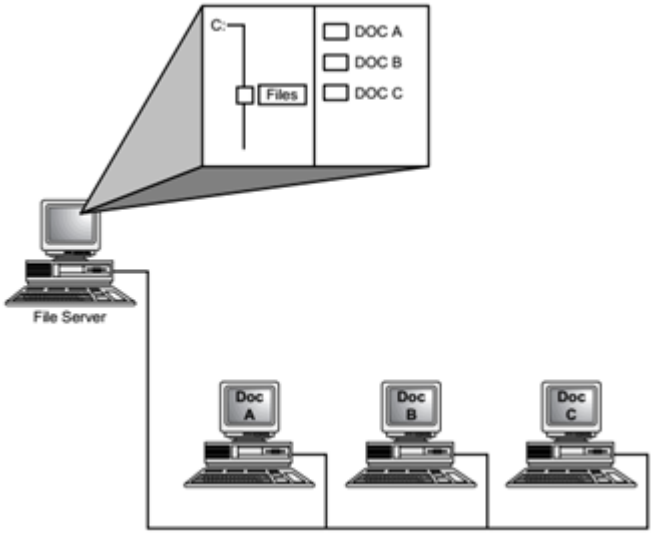
Some examples of client/server-based networks are Novell NetWare,Windows NT Server, and Windows Server 2003/2008. Some common server typesinclude file servers, mail servers, print servers, fax servers, and application servers. In a client/server network, the server machines oftenare not even set up to do the tasks that a client machine can do. (Ona Novell server, for example, a person cannot run aspreadsheet from the server console. Other systems, such asWindows NT and UNIX machines, enable a person to do this eventhough it is not the intended use of the system).

1.3 Network Services

Network services are the basic reason we connect computers. Servicesare what a company wants to have performed or provided. Based onthe services a company wants to utilize, the company purchases aspecific program and operating system. This section describes someof the most common services available on computer networks

1.3.1 File service

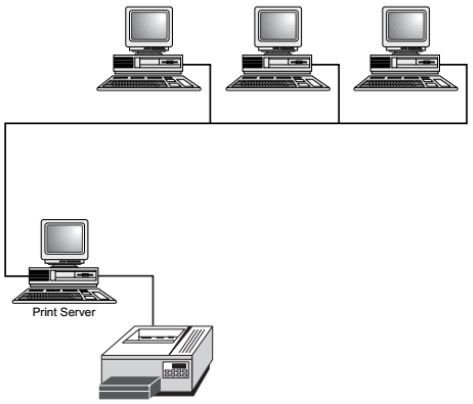
File services enable networked computers to share files with eachother. This capability was one of the primary reasons networking ofpersonal computers initially came about. File services include all network functions dealing with the storage, retrieval, or movement ofdata files. File services enable users to read, write, and manage filesand data. This includes moving files between computers and archiving files and data.This section begins by defining file services and then moves on toother related topics such as file transfers, file storage, data migration,file archiving, and file update synchronization.



File services are an important part of client/server and peer-to-peernetworks. Computers providing files services are referred to as fileservers (see Figure). Two types of servers exist: dedicated andnon-dedicated. Dedicated servers do nothing but fulfil requests tonetwork clients. These servers commonly are found in client/serverenvironments. Non-dedicated servers do double duty. They enable auser to go onto the machine acting as a file server and request theuse of files from other machines; at the same time, they give files tousers who request them from other computers on the network (seeFigure). Non-dedicated file servers often are found in peer-topeer networks. An example of a non-dedicated server is a Windows95 machine that accesses files from other computers on the networkand that provides access to its hard drive for other computers

1.3.2 Print service

After file services, printing is probably the second biggest incentivefor installing a LAN. The following are some of the many advantagesof network print services:Many users can share the same printers. This capability is especially useful with expensive devices such as colour printers andplotters.Printers can be located anywhere, not just next to a user's PC.Queue-based network printing is more efficient than directprinting because the workstation can begin to work again assoon as a job is queued to the network.Modern printing services enable users to send facsimile (fax)transmissions through the network to a fax server. Here, print services are defined as a network service that controls and manages access to printers and plotters (see Figure).



1.3.3 Communication service

Messaging/communication services generally transfer information fromone place to another. This communication of information can bebroken down into three subareas:

Email: Email systems can service any size group from a local workgroupto a corporation to the world. By installing email routing devices,you can transfer mail smoothly and efficiently among several LANs.Email also can be routed to and received from the Internet. Thisenables users in dozens of countries throughout the world toexchange electronic messages.

Voice mail: Voice mail enables you to connect your computer to a telephone system and to incorporate telephone voicemail messages with your PC.The technical term for this is telephony. This often involves movingyour voicemail messages from the phone system to the LAN andenabling the computer network to distribute this information to different clients.

Fax services: Fax services enable you to send or receive faxes from your computer.This is similar to printing in that you can "print" the document toa fax device. Fax services, however, can take on more complicatedfeatures including the capability to send faxes to a central fax serverand to receive faxes from the phone system to a central fax device.That device then delivers the fax message to your PC. This all occursautomatically.

1.3.4 Database service

Database servers are the most common type of application servers.Because database services enable applications to be designed in separate client and server components, such applications frequently arecalled client/server databases.With a client/server database, the client and server applications aredesigned to take advantage of the specialized capabilities of clientand database systems, as described here:The client application manages data input from the user, generation of screen displays, some of the reporting, and dataretrieval requests sent to the database server.The database server manages the database files; adds, deletes,and modifies records in the database; queries the database andgenerates the results required by the client; and transmitsresults back to the client. The database server can servicerequests for multiple clients at the same time.Database services relieve clients of most of the responsibilities formanaging data.

Microsoft SQL Server and Oracle are two examples of applicationsthat run at the server but are able to perform tasks requested byclients. Because of the way these applications were designed, bothrequire a back-end, or server, component and a front-end, or client,component.

1.3.4 Security service

Another service provided by networks is security. Security is one ofthe most important elements involved in a network. When usersshare resources and data on a network, they should be able to control who can access the data or resource and what the user can dowith it. An example of this is a file showing the financial records of acompany. If this file is on a file server, it is important to be able tocontrol who has access to the file. One step further, who is able toread and change the file also is a crucial consideration. This sameexample also applies to a shared printer. You might want to specifywho can use the expensive colour laser printer or, more specifically,when a person can use this printer. As you can see, security is animportant service on a network. Network administrators spend agreat deal of time learning and setting up security.

Security services often deal with a user account database or something like the aforementioned directory services. This database ofusers often contains a list of names and passwords. When a personwants to access the network, he must log on to the network.Logging on is similar to trying to enter an office building with asecurity guard at the front door. Before you can enter the building,you must verify who you are against a list of people who are allowedaccess.Security services often are intermingled with other services. Someservices added to a network can utilize the security services of thesystem onto which they have been installed. An example of this isMicrosoft Exchange Server. This messaging product can utilize thesecurity services of an existing Windows NT Server. An example of aproduct that does not need to utilize an existing security system isLotus Notes. Lotus Notes has its own independent security system

1.3.6 Application service

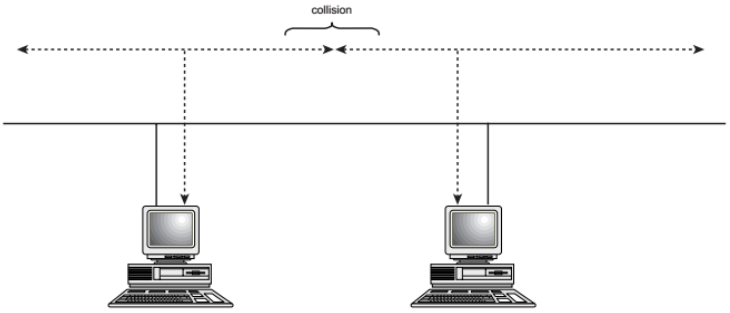
Application services enable applications to leverage the computingpower and specialized capabilities of other computers on a network.Business applications, for example, often must perform complex statistical calculations beyond the scope of most desktop PCs. Statisticalsoftware with the required capabilities might need to run on a mainframe computer or on a minicomputer. The statistical package, however, can make its capabilities available to applications on users' PCsby providing an application service.The client PC sends the calculation request to the statistics server.When the results become available, they are returned to the client.This way, only one computer in an organization needs to have theexpensive software license and processing power required to calculatethe statistics, but all client PCs can benefit.

Application services enable organizations to install servers that arespecialized for specific functions. Some of the morecommon application servers are database servers, messaging/communication servers, groupware servers, and directory servers.

1.4 Network Access Methods

An access method is a set of rules governing how the network nodesshare the transmission medium. The rules for sharing among computers are similar to the rules for sharing among humans in thatthey both boil down to a pair of fundamental philosophies:1) first come, first served and 2) take turns. These philosophies are theprinciples defining the three most important types of media accessmethods:

1.4.1 Contention



In its purest form, contention means that the computers are contending for use of the transmission medium.Any computer in the network can transmit at any time (firstcome, first served).In pure contention-based access control, any computer can transmitat any time. This system breaks down when two computers attemptto transmit at the same time, in which case a collision occurs (see Figure). Eventually,

when a network gets busy enough, mostattempts to transmit result in collisions and little effective communication can take place.Mechanisms are usually put into place to minimize the number ofcollisions. One mechanism is carrier sensing, whereby each computerlistens to the network before attempting to transmit. If the networkis busy, the computer refrains from transmitting until the networkquiets down. This simple “listen before talking” strategy can significantly reduce collisions.

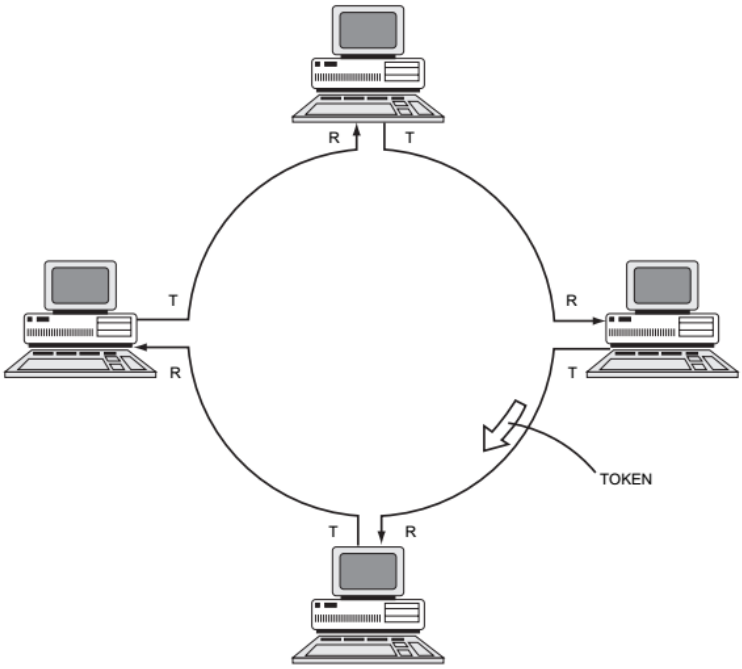
Another mechanism is carrier detection. With this strategy, computers continue to listen to the network as they transmit. If a computerdetects another signal that interferes with the signal it’s sending, itstops transmitting. Both computers then wait a random amount oftime and attempt to retransmit. Unless the network is extremelybusy, carrier detection along with carrier sensing can manage a largevolume of transmissions. Carrier detection and carrier sensing used together form the protocol used in all types of Ethernet: **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**. CSMA/CD limits the size of thenetwork to 2,500 meters. At longer distances, the broadcast-sensingmechanisms don’t work—a node at one end can’t sense when a nodeat the other end starts to broadcast.

Apple’s LocalTalk network uses the protocol **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**. Collision avoidance uses additionaltechniques to further reduce the likelihood of collisions. InCSMA/CA, each computer signals a warning that says it is about totransmit data, and then the other computers wait for the broadcast.CSMA/CA adds an extra layer of order, thereby reducing collisions,but the warning broadcasts increase network traffic, and the task ofconstantly listening for warnings increases system load.

CSMA/CD can be compared to trying to walk across the street andalmost being hit by a car. If you are almost hit by a car, then youwait a few moments before trying to cross again. CSMA/CA is similar, but in this case you send your friend across the street first. Ifyour friend is almost hit by a car, then you wait. If a car does not hithim, then you proceed.

1.4.2 Token passing

Token passing utilizes a frame called a token, which circulates aroundthe network. A computer that needs to transmit must wait until itreceives the token, at which time the computer is permitted to transmit. When the computer is done transmitting, it passes the tokenframe to the next station on the network. Figure shows howtoken passing is implemented on a token-ring network. Token-ringnetworks are discussed in greater detail later in this chapter in thesection titled “Token Ring.”



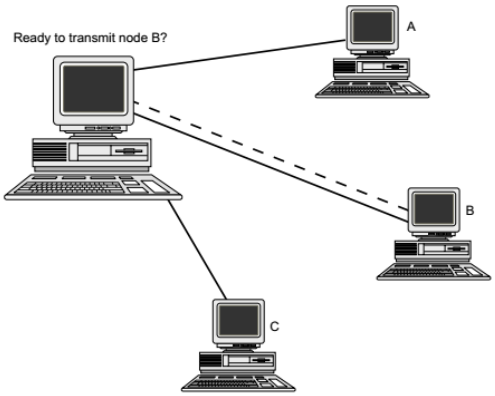
Several network standards employ token passing access control:Token ring. The most common token-passing standard,embodied in IEEE standard 802.5.IEEE standard 802.4. Implemented infrequently; defines a busnetwork that also employs token passing. ARCNet can deploythis standard, as is shown later in the chapter in the sectiontitled “ARCNet.”FDDI. A 100Mbps fibre-optic network standard that usestoken passing and rings in much the same manner as 802.5token ring.

Token-passing methods can use station priorities and other methodsto prevent any one station from monopolizing the network. Becauseeach computer has a chance to transmit each time the token

travelsaround the network, each station is guaranteed a chance to transmitat some minimum time interval.Token passing is more appropriate than contention under the following conditions:When the network is carrying time-critical data. Because tokenpassing results in more predictable delivery, token passing iscalled deterministic.When the network experiences heavy utilization. Performancetypically falls off more gracefully with a token-passing networkthan with a contention-based network. Token-passing networks cannot become gridlocked due to excessive numbers ofcollisions.When some stations should have higher priority than others. Sometoken-passing schemes support priority assignments.

1.4.3 Polling

Polling-based systems require a device (called a controller, or masterdevice) to poll other devices on the network to see whether they areready to either transmit or receive data as seen in Figure. Thisaccess method is not widely used on networks because the pollingitself can cause a fair amount of network traffic. A common exampleof polling is when your computer polls its printer to receive a printjob.



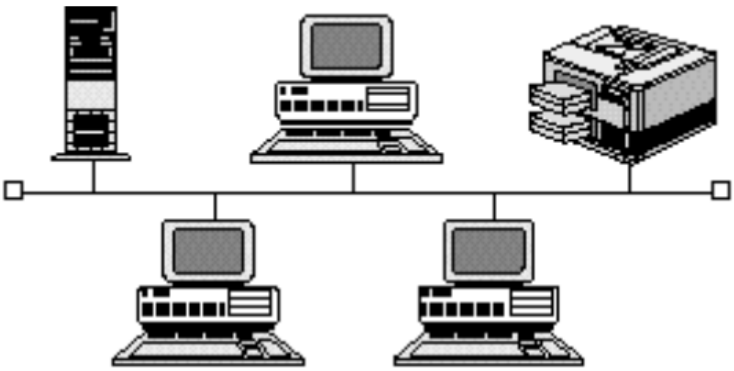
1.5 Network Topologies

A topology defines the arrangement of nodes, cables, and connectivity devices that make up the network. Two categories form the basisfor all discussions of topologies:Physical topology. Describes the actual layout of the networktransmission media.Logical topology. Describes the logical pathway a signal followsas it passes among the network nodes.Another way to think about this distinction is that a physical topology defines the way the network looks, and a logical topology definesthe way the data passes among the nodes. At a glance this distinctionmay seem nit-picky, but as you will learn in this chapter, the physicaland logical topologies for a network can be very different. A networkwith a star physical topology, for example, may actually have a busor a ring logical topology.

In common usage, the word “topology” applies to a complete network definition, which includes the physical and logical topologiesand also the specifications for elements such as the transmissionmedium. The term topology as used in Microsoft’s test objectives forthe Networking Essentials exam is not limited to the physical andlogical topology archetypes (that is, the design or layout) describedin this section

1.5.1 Bus

A bus physical topology is one in which all devices connect to a common, shared cable (sometimes called the backbone). A bus physical topology is shown in figure.If you think the bus topology seems ideally suited for the networksthat use contention-based access methods such as CSMA/CD, youare correct. Ethernet, the most common contention-based network architecture, typically uses bus as a physical topology.10BASE-T Ethernet networks (described later in this chapter) usebus as a logical topology but are configured in a star physical topology.

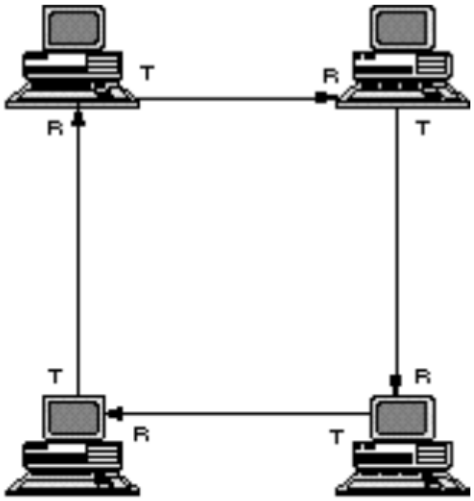


Most bus networks broadcast signals in both directions on thebackbone cable, enabling all devices to directly receive the signal.Some buses, however, are unidirectional: signals travel in only onedirection and can reach only downstream devices. A special connector calleda terminator must be placed at the end of

the backbone cable toprevent signals from reflecting back on the cable and causinginterference. In the case of a unidirectional bus, the cable must beterminated in such a way that signals can reflect back on the cableand reach other devices without causing disruption.

1.5.2 Ring

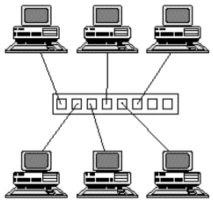
Ring topologies are wired in a circle. Each node is connected toits neighbours on either side, and data passes around the ring in one direction only (see fig.). Each device incorporates a receiver and a transmitter and serves as a repeater that passes thesignal on to the next device in the ring. Because the signal is regenerated at each device, signal degeneration is low.



Ring topologies are ideally suited for token-passing access methods. The token passes around the ring, and only the node thatholds the token can transmit data.Ring physical topologies are quite rare. The ring topology is almost always implemented as a logical topology. Token Ring, forexample—the most widespread token-passing network—alwaysarranges the nodes in a physical star (with all nodes connecting toa central hub) but passes data in a logical ring

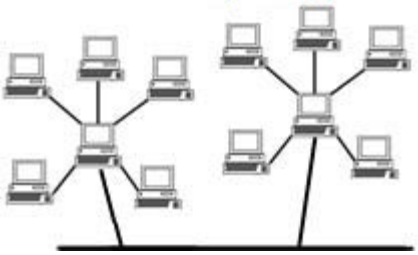
1.5.3 Star

Star topologies require that all devices connect to a central hub (see fig.). The hub receives signals from other network devicesand routes the signals to the proper destinations. Star hubs can beinterconnected to form tree or hierarchical network topologies.As mentioned earlier, a star physical topology is often used to implement a bus or ring logical topology.



1.5.4 Tree

A tree topology is a special type of structure in which many connected elements are arranged like the branches of a tree. For example, tree topologies are frequently used to organize the computers in a corporate network, or the information in a database.In a tree topology, there can be only one connection between any two connected nodes. Because any two nodes can have only one mutual connection, tree topologies form a natural parent and child hierarchy.



1.5.5 Hybrid (Mess)

A hybrid topology is a type of network topology that uses two or more differing network topologies. These topologies include a mix of bus topology, ring topology, star topology, and tree topology.

1.6 Advanced Network Topologies

1.6.1 Ethernet

Ethernet is an array of networking technologies and systems used in local area networks (LAN), where computers are connected within a primary physical space. Systems using Ethernet communication divide data streams into packets, which are known as frames. Frames include source and destination address information, as well as mechanisms used to detect errors in transmitted data and retransmission requests.

Ethernet transmission speeds are constantly improving and evolving. For example, 100BASE-TX and 1000BASE-T reference the physical Ethernet layer, which contains twisted pair cables and 8 Position 8 Contact (8P8C) modular connectors with male plugs and female jacks. These run at 100 Mbps and 1 Gbps, respectively. 100BASE-TX is also known as Fast Ethernet, where more common coaxial cables are replaced

by twisted pair cables, enabling faster frame transmissions. Carrier Ethernet is a high-bandwidth technology used for Internet access and connectivity by government, business and academic LANs.

1.6.2 CDDI (Copper Data Distribution Interface)

The logical topology used in CDDI is a ring-based token network. CDDI does not use the IEEE 802.5 Token Ring Protocol, but derives from the IEEE 802.4 Token Bus Timed Token Protocol. This network can support thousands of users or terminals as well as cover a wide geographical area. CDDI is not widely applied due to the decrease in the price of fiber optic installation, which has greater efficiency, a much higher bandwidth and an immunity to interference. Data transfer in CDDI has a throughput of 100 Mbps when using a redundancy architecture.

CDDI is the same networking system as FDDI, although the medium for the transmission is copper twisted-pair wire instead of fiber optic cables. Copper cables are no longer widely used because they can only stretch as far as 100 meters, compared to 1,000 meters for fiber optic cables. CDDI is commonly implemented in a wide geographical area.

1.6.3 FDDI (Fiber Distributed Data Interface)

FDDI networks, which are designed for geographically large-scaled organizations that support thousands of end users, operates in the OSI model's physical and media access control (MAC layers). The American National Standards Committee (ANSC) formally standardized FDDI as the best linking medium for local area networks (LAN), which use FDDI for long-distance communication.

FDDI also is used by single and multi-mode fiber optic, which have different communication mechanisms. Multi-mode fiber optic uses a lead generation device, whereas single-mode fiber optic uses laser for data transmission only.

1.7 Communication Methods

1.7.1 Unicasting

Unicast is the term used to describe communication where a piece of information is sent from one point to another point. In this case there is just one sender, and one receiver. Unicast transmission, in which a packet is sent from a single source to a specified destination, is still the predominant form of transmission on LANs and within the Internet. All LANs (e.g. Ethernet) and IP networks support the unicast transfer mode, and most users are familiar with the standard unicast applications (e.g. http, smtp, ftp and telnet) which employ the TCP transport protocol.

1.7.2 Multicasting

Multicast is the term used to describe communication where a piece of information is sent from one or more points to a set of other points. In this case there is may be one or more senders, and the information is distributed to a set of receivers (there may be no receivers, or any other number of receivers). One example of an application which may use multicast is a video server sending out networked TV channels. Simultaneous delivery of high quality video to each of a large number of delivery platforms will exhaust the capability of even a high bandwidth network with a powerful video clip server. This poses a major scalability issue for applications which required sustained high bandwidth. One way to significantly ease scaling to larger groups of clients is to employ multicast networking.

Multicasting is the networking technique of delivering the same packet simultaneously to a group of clients. IP multicast provides dynamic many-to-many connectivity between a set of senders (at least 1) and a group of receivers. The format of IP multicast packets is identical to that of unicast packets and is distinguished only by the use of a special class of destination address (class D IPv4 address) which denotes

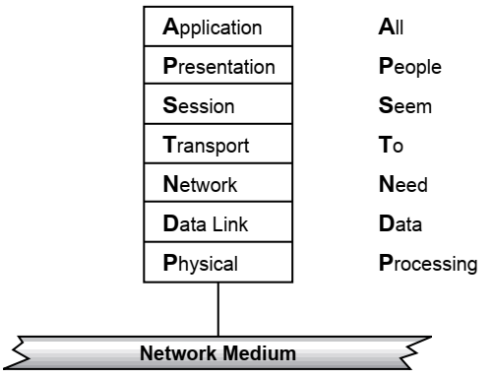
a specific multicast group. Since TCP supports only the unicast mode, multicast applications must use the UDP transport protocol.

1.7.3 Broadcasting

Broadcast is the term used to describe communication where a piece of information is sent from one point to all other points. In this case there is just one sender, but the information is sent to all connected receivers. Broadcast transmission is supported on most LANs (e.g. Ethernet), and may be used to send the same message to all computers on the LAN (e.g. the address resolution protocol (arp) uses this to send an address resolution query to all computers on a LAN). Network layer protocols (such as IPv4) also support a form of broadcast that allows the same packet to be sent to every system in a logical network (in IPv4 this consists of the IP network ID and an all 1's host number).

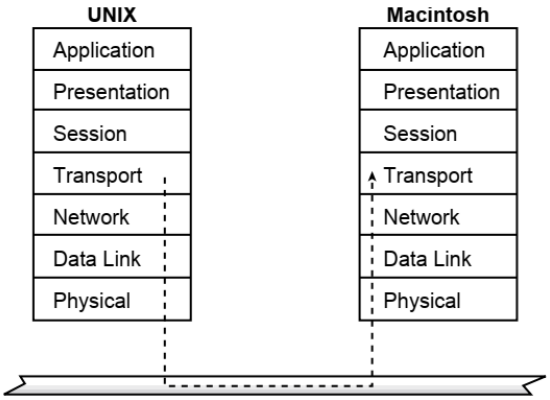
1.8 OSI reference model with 7 layers

The most commonly used model is the Open Systems Interconnection (OSI) reference model. The OSI model, first released in 1984 by the International Standards Organization (ISO), provides a useful structure for defining and describing the various processes underlying open systems networking. The OSI model is a blueprint for vendors to follow when developing protocol implementations. The OSI model organizes communication protocols into seven layers. Each layer addresses a narrow portion of the communication process. Figure illustrates the layers of the OSI model.



Although you will examine each layer in detail later, a quick overview is in order. Layer 1, the Physical layer, consists of protocols that control communication on the network media. Layer 7, the Application layer, interfaces the network services with the applications in use on the computer. The five layers between Data Link, Network, Transport, Session, and Presentation perform intermediate communication tasks.

Two computers must run compatible protocol stacks before they can communicate because each layer in one computer's protocol stack must interact with a corresponding layer in the other computer's protocol stack. Figure, for example, shows the path of message that starts in the Transport layer. The message travels down the protocol stack, through the network medium, and up the protocol stack of the receiving computer. If the Transport layer in the receiving computer understands the protocols used in the Transport layer that originated the message, the message can be delivered.



1.8.1 OSI Physical Layer Concepts

Although the OSI Physical layer does not define the media used, this layer is concerned with all aspects of transmitting and receiving data on the network media. Specifically, the Physical layer is concerned with

transmitting and receiving bits. This layer defines several key characteristics of the physical network, including the following:

- Physical structure of the network (physical topology)
- Mechanical and electrical specifications for using the medium (not the medium itself)
- Bit transmission encoding and timing

Although the Physical layer does not define the physical medium, it defines clear requirements that the medium must meet. These specifications differ depending on the physical medium. Ethernet for UTP, for example, has different Physical layer specifications from coaxial Ethernet.

1.8.2 OSI Data Link Layer Concepts

As you learned in the preceding section, the OSI Physical layer is concerned with moving messages at the machine level. Network communication, however, is considerably more involved than moving bits from one device to another. In fact, dozens of steps must be performed to transport a message from one device to another. Real messages consist not of single bits but of meaningful groups of bits. The Data Link layer receives messages, called frames, from upper layers. A primary function of the Data Link layer is to disassemble these frames into bits for transmission and then to reconstruct the frames from the bits received.

The Data Link layer has other functions as well, such as addressing, error control, and flow control for a single link between network devices. (The adjacent Network layer, described later in this chapter, handles the more complex tasks associated with addressing and delivering packets through routers and across an internetwork.) The IEEE 802 standard divides the Data Link layer into two sublayers:

> **Media Access Control (MAC)**. The MAC sublayer controls the means by which multiple devices share the same media channel. This includes contention methods, and other media access details. The MAC layer also provides addressing information for communication between network devices.
>
> **Logical Link Control (LLC).** The LLC sublayer establishes and maintains links between communicating devices.

The Data Link layer maintains device addresses that enable messages to be sent to a particular device. The addresses are called physical device addresses. Physical device addresses are unique addresses associated with the networking hardware in the computer. In most cases (for example, Ethernet and Token Ring), the physical device address is burned into the network interface card at the time the card is manufactured.

The standards that apply to a particular network determine the format of the address. Because the address format is associated with the media access control method used, physical device addresses are frequently referred to as MAC addresses.

1.8.3 OSI Network Layer Concepts

As you learned in the preceding section, the Data Link layer deals with communication between devices on the same network. Physical device addresses are used to identify data frames, and each device is responsible for monitoring the network and receiving frames addressed to that device. The Network layer handles communication with devices on logically separate networks that are connected to form internetworks.

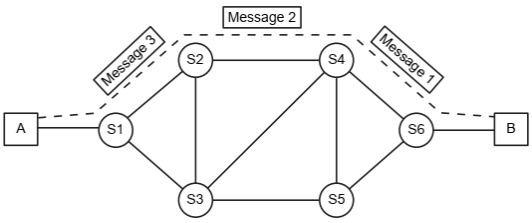
Because internetworks can be large and can be constructed of different types of networks, the Network layer utilizes routing algorithms that guide packets from their source to their destination networks. For more about routing and routing algorithms. You have already encountered the Data Link layer's physical device addresses, which uniquely identify each device on a network. On larger networks, it is impractical to deliver network data solely by means of physical addresses. (Imagine if your network adapter had to check

every packet sent from anywhere on the Internet to look for a matching physical address.) Larger networks require a means of routing and filtering packets in order to reduce network traffic and minimize transmission time. The Network layer uses logical network addresses to route packets to specific networks on an internetwork. Logical network addresses are assigned during configuration of the networks. A network installer must make sure that each network address is unique on a given internetwork.

Delivering Packets: Many internetworks often include redundant data paths that you can use to route messages. Typically, a packet will pass from the local LAN segment of the source PC through a series of routers to the local LAN segment of the destination PC. The OSI Network layer oversees the process of determining paths and delivering packets across the internetwork. Chapter 6 describes some of the routing algorithms used to determine a path. The following sections introduce some of the basic switching techniques, as follows:

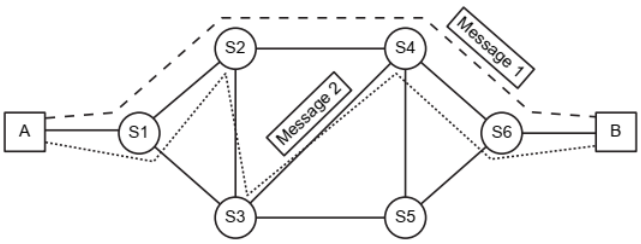
- Circuit switching
- Message switching
- Packet switching

Circuit Switching: Circuit switching establishes a path that remains fixed for the duration of a connection (see fig.). Much as telephone switching equipment establishes a route between two telephones, circuit switching networks establish a path through the internetwork when the devices initiate a conversation. These paths tend to be reliable and fast in performance.



Circuit switching provides devices with a dedicated path and a well-defined bandwidth, but circuit switching is not free of disadvantages. First, establishing a connection between devices can be time-consuming. Second, because other traffic cannot share the dedicated media path, bandwidth might be inefficiently utilized. This can be compared to having a telephone conversation, yet not speaking. You are using the line, thus not allowing others to use it, but you are not transmitting any data. Finally, circuit-switching networks must have a surplus of bandwidth, so these types of switches tend to be expensive to construct.

Message Switching: Message switching treats each message as an independent entity. Each message carries address information that describes the message's destination, and this 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 messages to their destinations.

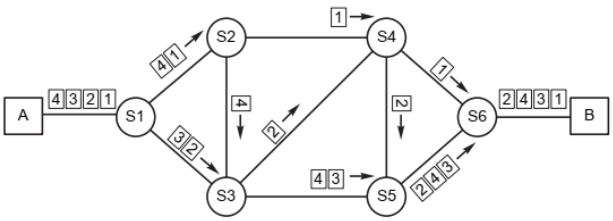


Message switches also may be programmed with information about the most efficient routes. Depending on network conditions, different messages may be sent through the network by different routes, as shown in Figure. Message switching transfers the complete message from one switch to the next, where the message is stored before being forwarded again. Because each message is stored before being sent on to the next switch, this type of network frequently is called a store-and forward network. The message switches often are general-purpose computers and must be equipped with sufficient storage (usually hard drives, or RAM) to enable them to store messages until forwarding is possible. Message switching is commonly used in email because some delay is permissible in the delivery of email. Message switching uses relatively low-cost devices to forward messages and can

function well with relatively slow communication channels. Other applications for message switching include group applications such as workflow, calendaring, and groupware. Message switching offers the following advantages:

- Data channels are shared among communicating devices, improving the efficiency of available bandwidth.
- Message switches can store messages until a channel becomes available, reducing sensitivity to network congestion.
- Message priorities can be used to manage network traffic.
- Broadcast addressing uses network bandwidth more efficiently by delivering messages to multiple destinations.

Packet Switching: In packet switching, messages are divided into smaller pieces called packets. Each packet includes source and destination address information so that individual packets can be routed through the internetwork independently. As you can see in Figure, the packets that make up a message can take very different routes through the internetwork. So far, packet switching looks considerably like message switching, but the distinguishing characteristic is that packets are restricted to a size that enables the switching devices to manage the packet data entirely in memory. This eliminates the need for switching devices to store the data temporarily on disk. Packet switching, therefore, routes packets through the network much more rapidly and efficiently than is possible with message switching. Several methods of packet switching exist. Two common methods of packet switching are as: Datagram and Virtual circuit.



1.8.4 OSI Transport Layer Concepts

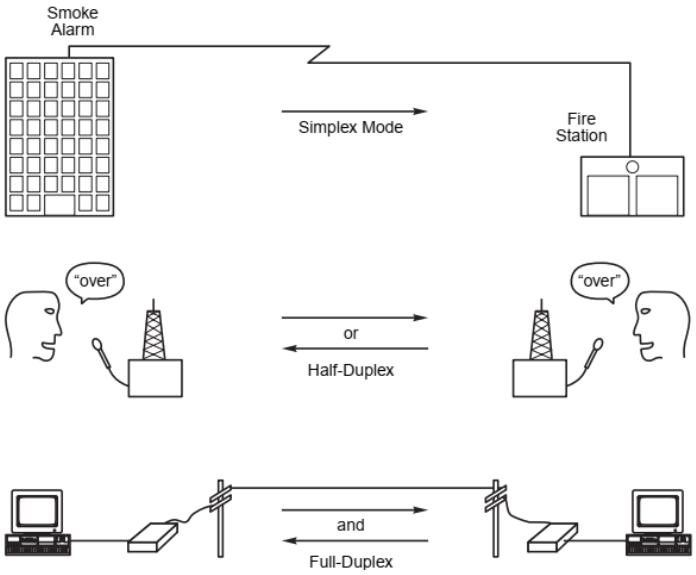
The Transport layer, the next layer of the OSI model, can implement procedures to ensure the reliable delivery of messages to their destination devices. The term “reliable” does not mean that errors cannot occur; instead, it means that if errors occur, they are detected. If errors such as lost data are detected, the Transport layer either requests retransmission or notifies upper-layer protocols so that they can take corrective action. The Transport layer enables upper-layer protocols to interface with the network but hides the complexities of network operation from them. One of the functions of the Transport layer is to break large messages into segments suitable for network delivery.

Some services can be performed at more than one layer of the OSI model. In addition to the Data Link and Network layers, the Transport layer can take on some responsibility for connection services. The Transport layer interacts with the Network layer’s connection-oriented and connectionless services and provides some of the essential quality control features. Some of the Transport layer’s activities include the following:

- Repackaging. When large messages are divided into segments for transport, the Transport layer must repackage the segments when they are received before reassembling the original message.
- Error control. When segments are lost during transmission or when segments have duplicate segment IDs, the Transport layer must initiate error recovery. The Transport layer also detects corrupted segments by managing end-to-end error control using techniques such as checksums.
- End-to-end flow control. The Transport layer uses acknowledgments to manage end-to-end flow control between two connected devices. Besides negative acknowledgments, some Transport layer protocols can request the retransmission of the most recent segments.

1.8.5 OSI Session Layer Concepts

The next OSI layer, the Session layer, manages dialogs between two computers by establishing, managing, and terminating communications. As illustrated in Figure, dialogs can take three forms:



- **Simplex dialogs**. These dialogs are responsible for one-way data transfers only. An example is a fire alarm, which sends an alarm message to the fire station but cannot (and does not need to) receive messages from the fire station.
- **Half-duplex dialogs**. These dialogs handle two-way data transfers in which the data flows in only one direction at a time. When one device completes a transmission, this device must "turn over" the medium to the other device so that this second device has a turn to transmit. In a similar fashion, CB radio operators converse on the same communication channel. When one operator finishes transmitting, he must release his transmit key so that the other operator can send a response.
- **Full-duplex dialogs**. This third type of dialog permits two-way simultaneous data transfers by providing each device with a separate communication channel. Voice telephones are fullduplex devices, and either party to a conversation can talk at any time. Most computer modems can operate in full-duplex mode.

Costs rise for half- and full-duplex operation because the more complex dialog technologies are naturally more expensive. Designers of communications systems, therefore, generally use the simplest dialog mode that satisfies the communication requirements. Half-duplex communication can result in wasted bandwidth during the intervals when communication is turned around. On the other hand, using full-duplex communication generally requires a greater bandwidth than half-duplex communication. The Session layer also marks the data stream with checkpoints and monitors the receipt of those checkpoints. In the event of a failure, the sending PC can retransmit, starting with the data sent after the last checkpoint, rather than resend the whole message.

1.8.6 OSI Presentation Layer Concepts

The Presentation layer deals with the syntax, or grammatical rules, needed for communication between two computers. The Presentation layer converts system-specific data from the Application layer into a common, machine-independent format that supports amore standardized design for lower protocol layers. The Presentation layer also attends to other details of data formatting, such as data encryption and data compression. On the receiving end, the Presentation layer converts the machine independent data from the network into the format required for the local system. This conversion could include the following:

Data formatting. This is the organization of the data. This topic is actually broken down into four subtopics:

- Bit-order translation. When binary numbers are transmitted through a network, they are sent one bit at a time. The transmitting computer can start at either end of the number. Some computers start at the most significant digit (MSD); others start at the least significant digit (LSD). Essentially this has to do with whether information is read from right to left or from left to right.
- Byte-order translation. Complex values generally must be represented with more than one byte, but different computers use different conventions to determine which byte should be transmitted first. Intel microprocessors, for example, start with the least significant byte and are

called little endian. Motorola microprocessors, on the other hand, start with the most significant byte and are called big endian. Byte-order translation might be needed to reconcile these differences when transferring data between a computer with an Intel processor and a Motorola processor.

- Character code translation. Different computers use different binary schemes for representing character sets. For instance: ASCII, the American Standard Code for Information Interchange, is used to represent English characters on all microcomputers and most minicomputer; EBCDIC, the Extended Binary Coded Decimal Interchange Code, is used to represent English characters on IBM mainframes; and Shift-JIS is used to represent Japanese characters.
- File syntax translation. File formats differ between computers. For instance, Macintosh files actually consist of two:

Encryption. Encryption puts data into a form unreadable by unauthorized users. Encryption takes on two main forms:

- Public key. This uses a rule of encryption (the key) and a known value. The manipulation of the key with a known value produces a mechanism for decrypting data.
- Private Key. This encryption uses one key. All components that have the key can decrypt the data. The redirector service operates at the OSI Presentation layer.

1.8.7 OSI Application Layer Concepts

The Application layer of the OSI reference model is concerned with providing services on the network, including file services, print services, application services such as database services, messaging services, and directory services among others. A common misunderstanding is that the Application layer is responsible for running user applications such as word processors. This is not the case. The Application layer, however, does provide an interface whereby applications can communicate with the network. It isthis interface that is often referred to as the Application Programming Interface (API). Some examples of APIs include MAPI (Messaging Programming Interface) and TAPI (Telephony Application Programming Interface).

The Application layer also advertises the available services that your computer has to the network. An example of this is when you double-click on the Network Neighbourhood Icon in Windows 95 or Windows NT. The resulting picture shows a list of computers that have services available to network users. (The security service of these computers determines whether or not a user has access.) The nature of these services is beyond the scope of this chapter. In general, you would take a course or read a book to understand how to manage different services on a network. Examples of these services include Windows NT security, file and printing management, SMTP mail, fax servers, and ODBC connectivity. This book covers some of the basics of Windows NT Security, “Managing and Securing a Microsoft Network.

1.9 TCP/IP network model with 4 layers

The OSI Model we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defence (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

The diagrammatic comparison of the TCP/IP and OSI model is as follows:

TCP/IP	OSI Model	Protocols
Application Layer	Application Layer	DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP, POP3, RTP, RTSP, SSH, SIP, SMTP, SNMP, Telnet, TFTP
	Presentation Layer	JPEG, MIDI, MPEG, PICT, TIFF
	Session Layer	NetBIOS, NFS, PAP, SCP, SQL, ZIP
Transport Layer	Transport Layer	TCP, UDP
Internet Layer	Network Layer	ICMP, IGMP, IPsec, IPv4, IPv6, IPX, RIP
Link Layer	Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring
	Physical Layer	Bluetooth, Ethernet, DSL, ISDN, 802.11 Wi-Fi

1.9.1. Network Access Layer (Link Layer)

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data. We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

1.9.2. Internet Layer

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are:

- **IP** – stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
- **ICMP** – stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
- **ARP** – stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

1.9.3. Transport Layer (Host-to-Host Layer)

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are:

- **Transmission Control Protocol (TCP)** – It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
- **User Datagram Protocol (UDP)** – On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

4. Application Layer (Process Layer)

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications.

Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are:

- **HTTP and HTTPS – HTTP stands for Hypertext transfer protocol**. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
- **SSH – SSH stands for Secure Shell**. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
- **NTP – NTP stands for Network Time Protocol**. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

1.10 File And Print Sharing in LAN.

https://youtu.be/UvXL2F5Bymo

https://youtu.be/TTPnKG0v7w8

1.11 Mapping of network drive

https://youtu.be/xW_NHk3JcS4

1.12 Disk quota

A disk quota provides a fixed and limited amount of storage. Disk quotas are assigned to home directories, file shares and email mailboxes. By assigning quotas, no single user or area can consume enough space to cause an outage to the system or impact other users. You can check how much of your assigned quota you are using on file shares and home directories by looking at the size of the file share when it is mapped to a workstation. For example to check how much used and free space you have on your home directory while logged into a Windows workstation go to Computer, right click on your home directory and select Properties.

Once you reach your quota you will be unable to write any more data or files to the location and you may receive an error from the application you are using. If you reach your quota on your home directory you will also immediately be sent an email informing you that you have reached your quota and need to clean up files. You will also be sent a reminder email every 24 hours that you are over quota. If you reach your quota you should delete or archive any no longer used or old files to reduce the amount of space you are using.

https://youtu.be/mRmC1K-4zbQ

1.13 Encryption

In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating cipher text that can be read only if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption

scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

1.14 Compression

Compression is a reduction in the number of bits needed to represent data. Compressing data can save storage capacity, speed up file transfer, and decrease costs for storage hardware and network bandwidth. Compression is performed by a program that uses a formula or algorithm to determine how to shrink the size of the data. For instance, an algorithm may represent a string of bits -- or 0s and 1s -- with a smaller string of 0s and 1s by using a dictionary for the conversion between them, or the formula may insert a reference or pointer to a string of 0s and 1s that the program has already seen. Text compression can be as simple as removing all unneeded characters, inserting a single repeat character to indicate a string of repeated characters and substituting a smaller bit string for a frequently occurring bit string. Data compression can reduce a text file to 50% or a significantly higher percentage of its original size.

For data transmission, compression can be performed on the data content or on the entire transmission unit, including header data. When information is sent or received via the internet, larger files, either singly or with others as part of an archive file, may be transmitted in a ZIP, GZIP or other compressed format.

1.15 NetMeeting

Microsoft NetMeeting is a discontinued VoIP and multi-point videoconferencing client included in many versions of Microsoft Windows (from Windows 95 OSR2 to Windows XP). It uses the H.323 protocol for videoconferencing, and is interoperable with OpenH323-based clients such as Ekiga, OpenH323, and Internet Locator Service (ILS) as reflector. It also uses a slightly modified version of the T.120 Protocol for white boarding, application sharing (or by extension, desktop sharing), and file transfers.

NetMeeting was originally bundled with later versions of Internet Explorer 3, and with Internet Explorer 4. It incorporates technology acquired by Microsoft from UK software developer Data Connection Ltd and Data Beam Corporation (subsequently acquired by Lotus). Before video service became common on free IM clients, such as Yahoo! Messenger and MSN Messenger, NetMeeting was a popular way to perform video conferences and chatting over the Internet (with the help of public ILS servers, or "direct-dialing" to an IP address). The defunct TechTV channel even used NetMeeting as a means of getting viewers onto their call-in shows via webcam, although viewers had to call on their telephones, because broadband Internet connections were still rare.

https://youtu.be/HmJvXYKaq7g

https://youtu.be/Wjd7sJKDrEo

Unit-2

Transmission Media, Multiplexing and Switching Concepts, Network Devices

2.1 Transmission Media

On any network, the various entities must communicate through some form of media. Human communication requires some sort of media, whether it is technologically based (as are telephone wires) or whether it simply involves the use of our senses to detect soundwaves propagating through the air. Likewise, computers can communicate through cables, light, and radio waves. Transmission media enable computers to send and receive messages but, as in human communication, do not guarantee that the messages will be understood.

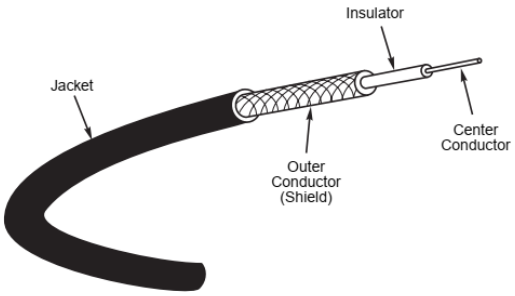
This chapter discusses some of the most common network transmission media. One broad classification of this transmission media is known as bounded media, or cable media. This includes cable types such as coaxial cable, shielded twisted-pair cable, unshielded twisted pair cable, and fiber-optic cable. Another type of media is known as boundless media; these media include all forms of wireless communications. To lay the groundwork for these issues, the chapter begin switch an introduction to the frequencies in the electromagnetic spectrum and a look at some important characteristics of the transmission media that utilize these different frequencies to transmit the data.

2.1.1 Guided Media (Network Cabling Media)

For the Networking Essentials, you need to know how to make decisions about network transmission media based on some of the factors described in previous sections of this chapter. The following sections discuss three types of network cabling media, as follows:

Coaxial Cable

Coaxial cables were the first cable types used in LANs. As shown in Figure, coaxial cable gets its name because two conductors sharea common axis; the cable is most frequently referred to as a "coax. "A type of coaxial cable that you may be familiar with is your television cable. The components of a coaxial cable are as follows:



- A center conductor, although usually solid copper wire, is sometimes made of stranded wire.
- An outer conductor forms a tube surrounding the center conductor. This conductor can consist of braided wires, metallic foil, or both. The outer conductor, frequently called the shield, serves 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

Types of Coaxial Cable

The two basic classifications for coaxial cable are as follows:

- Thinnet
- Thicknet

The following sections discuss Thinnet and Thicknet coaxial cabling.

Thinnet

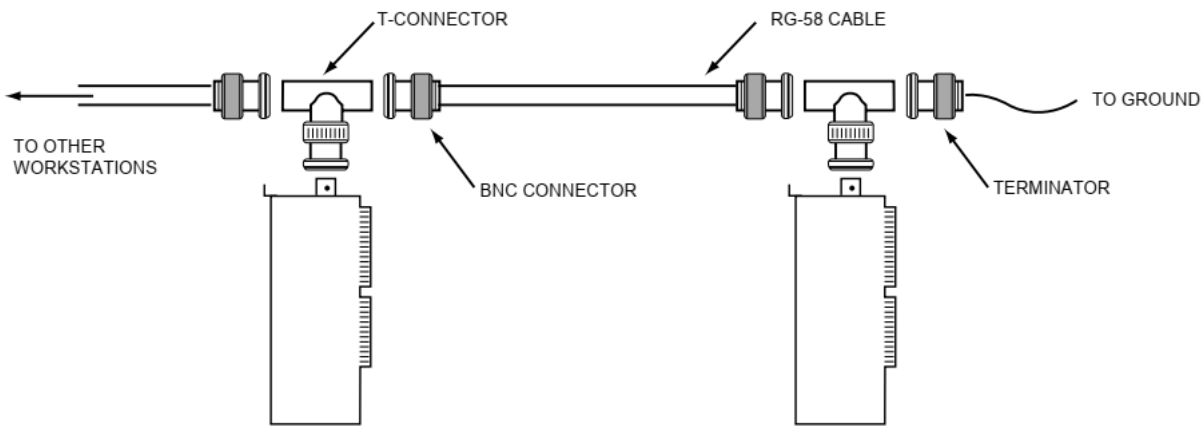
Thinnet is a light and flexible cabling medium that is inexpensiveand easy to install. Note that Thinnet falls under the RG-58 family, which has a 50-ohm impedance.Thinnet is approximately .25 inches (6 mm) inthickness.

Thicknet

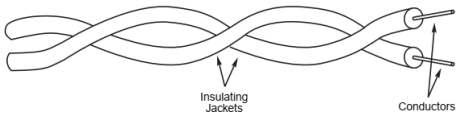
Thicknet (big surprise) is thicker than Thinnet. Thicknet coaxialcable is approximately 0.5 inches (13 mm) in diameter. Because it isthicker and does not bend as readily as Thinnet, Thicknet cable isharder to work

with. A thicker center core, however, means that Thicknet can carry more signals a longer distance than Thinnet. Thicknet can transmit a signal approximately 500 meters (1,650feet). Thicknet cable is sometimes called Standard Ethernet (although other cabling types described in this chapter are used for Ethernet also). 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. However, Thicknet can be installed relatively safely outside, running from building to building.

Installation



Twisted Pair Cable



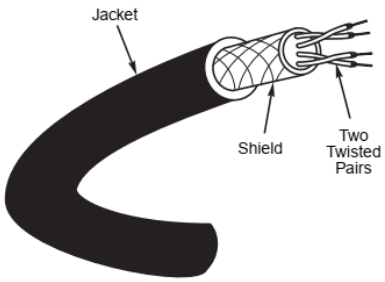
Twisted-pair cable has become the dominant cable type for all newnetwork designs that employ copper cable. Among the several reasons for the popularity of twisted-pair cable, the most significant isits low cost. Twisted-pair cable is inexpensive to install and offers thelowest cost per foot of any cable type. Your telephone cable is anexample of a twisted-pair type cable.

A basic twisted-pair cable consists of two strands of copper wire twisted together (see Figure). The twisting reduces the sensitivity of the cable to EMI and also reduces the tendency of the cable toradiate radio frequency noise that interferes with nearby cables andelectronic components, because the radiated signals from the twistedwires tend to cancel each other out. (Antennas, which are purposelydesigned to radiate radio frequency signals, consist of parallel, nottwisted, wires).

Twisting of the wires also controls the tendency of the wires in thepair to cause EMI in each other. As noted previously, whenever twowires are in close proximity, the signals in each wire tend to producecrosstalk in the other. Twisting the wires in the pair reduces crosstalkin much the same way that twisting reduces the tendency of thewires to radiate EMI.

A twisted-pair cable is used in most cases to connect a PC to either aHUB or a MAU. Two types oftwisted-pair cable are used in LANs: shielded and unshielded, asexplained in the following section.

Shielded Twisted-Pair (STP) Cable



Shielded twisted-pair cabling consists of one or more twisted pairs ofcables enclosed in a foil wrap and woven copper shielding. Figureshows IBM Type 1 cabling, the first cable type used with IBMToken Ring. Early LAN designers used shielded twisted-pair cablebecause the shield performed double duty, reducing the tendency ofthe cable to radiate EMI and reducing the cable's sensitivity to outside interference. Coaxial and STP cables use shields for the same purpose. The shieldis connected to the

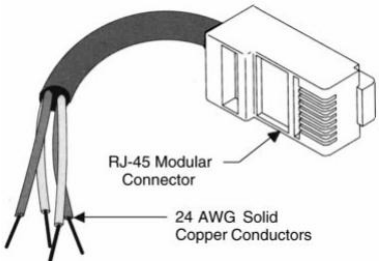
ground portion of the electronic device to whichthe cable is connected. A ground is a portion of the device thatserves as an electrical reference point, and usually, it is literally connected to a metal stake driven into the ground. A properly groundedshield prevents signals from getting into or out of the cable.

Unshielded Twisted-Pair (UTP) Cable

Unshielded twisted-pair cable doesn't incorporate a braided shieldinto its structure. However, the characteristics of UTP are similar inmany ways to STP, differing primarily in attenuation and EMI. Several twisted pairs can be bundled togetherin a single cable. These pairs are typically color-coded to distinguishthem.Telephone systems commonly use UTP cabling. Network engineerscan sometimes use existing UTP telephone cabling (if it is newenough and of a 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 noiseand susceptibility to EMI. Now, however, a clear trend toward UTPis in operation, and all new copper-based cabling schemes are basedon UTP.

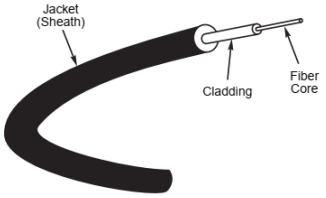
Connectors for UTP

The most common connector used with UTP cables is the RJ-45 (Registered Jack)connector shown in Figure. These connectors are easy to installon cables and are also extremely easy to connect and disconnect. AnRJ-45 connector has eight pins and looks like a common RJ-11 telephone connector. They are slightly different sizes, however, andwon't fit together: an RJ-11 has only four pins.



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 extremelyhigh bandwidths, but it also presents no problems with EMI andsupports durable cables and cable runs as long as several kilometers.The two disadvantages of fiber-optic cable, however, are cost andinstallation difficulty. Despite these disadvantages, fiber-optic cable isnow often installed into buildings by telephone companies as thecable of choice.



The center conductor of a fiber-optic cable is a fiber that consists ofhighly refined glass or plastic designed to transmit light signals withlittle loss. A glass core supports a longer cabling distance, but a plastic core is typically easier to work with. The fiber is coated with acladding or a gel that reflects signals back into the fiber to reducesignal loss. A plastic sheath protects the fiber (see Figure).A fiber-optic network cable consists of two strands separatelyenclosed in plastic sheaths. One strand sends and the other receives.Two types of cable configurations are available: loose and tightconfigurations. Loose configurations incorporate a space between thefiber sheath and the outer plastic encasement; this space is filled witha gel or other material. Tight configurations contain strength wiresbetween the conductor and the outer plastic encasement. In bothcases, the plastic encasement must supply the strength of the cable,while the gel layer or strength wires protect the delicate fiber frommechanical damage.

Optical fiber cables don't transmit electrical signals. Instead, the datasignals must be converted into light signals. Light sources includelasers and light-emitting diodes (LEDs). LEDs are inexpensive butproduce a fairly poor quality of light suitable for only less-stringentapplications.

The end of the cable that receives the light signal must convert thesignal 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 ariseswhen 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 extremeprecision to prevent excessive signal loss.

COMPARISON OF CABLE MEDIA

Cable Type	*Cost*	*Installation*	*Capacity*	*Range*	*EMI*
Coaxial Thinnet	Less than STP	Inexpensive/easy	10Mbps typical	185 m	Less sensitive than UTP
Coaxial Thicknet	Greater than STP, less than fiber	Easy	10Mbps typical	500 m	Less sensitive than UTP
Shielded twisted-pair (STP)	Greater than UTP, less than Thicknet	Fairly easy	16Mbps typical up to 500Mbps	100 m typical	Less sensitive than UTP
Unshielded twisted-pair (UTP)	Lowest	Inexpensive/easy	10Mbps typical up to 100Mbps	100 m typical	Most sensitive
Fiber-optic	Highest	Expensive/difficult	100Mbps typical	10s of kilometers	Insensitive

2.1.2 Unguided Media

The extraordinary convenience of wireless communications hasplaced an increased emphasis on wireless networks in recent years.Technology is expanding rapidly and will continue to expand intothe near future, offering more and better options for wireless networks.Presently, you can subdivide wireless networking technology intothree basic types corresponding 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 function as members of a cable-based LAN.
- 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. The following sections describe these technologies and some of the networking options available with each.

Reasons for Wireless Networks

Wireless networks are especially useful for the following situations:

- Spaces where cabling would be impossible or inconvenient. These include open lobbies, inaccessible parts of buildings, older buildings, historical buildings where renovation is prohibited, and outdoor installations.
- People who move around a lot within their work environment. Network administrators, for instance, must troubleshoot a large office network. Nurses and doctors need to make rounds at a hospital.
- Temporary installations. These situations include any temporary department set up for a specific purpose that soon will be torn down or relocated.
- People who travel outside of the work environment and need instantaneous access to network resources.
- Satellite offices or branches, ships in the ocean, or teams in remote field locations that need to be connected to a main office or location.

You can classify wireless LAN communications according to transmission method. The four most common LAN wireless transmissionmethods are as follows:

Infrared

You use an infrared communication system every time you controlyour television with a remote control. The remote control transmitspulses of infrared light that carry coded instructions to a receiver onthe TV. This technology also is used for network communication.

Four varieties of infrared communications are as follows:

- Broadband optical telepoint. This method uses broadband technology. Data transfer rates in this high-end option are competitive with those for a cable-based network.
- Line-of-sight infrared. Transmissions must occur over a clear line-of-sight path between transmitter and receiver.
- Reflective infrared. Wireless PCs transmit toward a common, central unit, which then directs communication to each of the nodes.
- Scatter infrared. Transmissions reflect off floors, walls, and ceilings until (theoretically) they finally reach the receiver. Because of the imprecise trajectory, data transfer rates are slow. The maximum reliable distance is around 100 feet. Infrared transmissions are typically limited to within 100 feet.

Within this range, however, infrared is relatively fast. Infrared's highbandwidth supports transmission speeds of up to 10Mbps.Infrared devices are insensitive to radio-frequency interference, butreception can be degraded by bright light. Because transmissions aretightly focused, they are fairly immune to electronic eavesdropping.Infrared transmissions are commonly used for LAN transmissions,yet can also be employed for WAN transmissions as well.

Leaser

High-powered laser transmitters can transmit data for several thousand yards when line-of-sight communication is possible. Lasers canbe used in many of the same situations as microwave links, but do not require an FCC license. On a LANscale, laser light technology is similar to infrared technology. Laserlight technology is employed in both LAN and WAN transmissions,though it is more commonly used in WAN transmissions.

Radio

There are two types of Radio transmission describe as follows:

Narrow-Band Radio Transmission

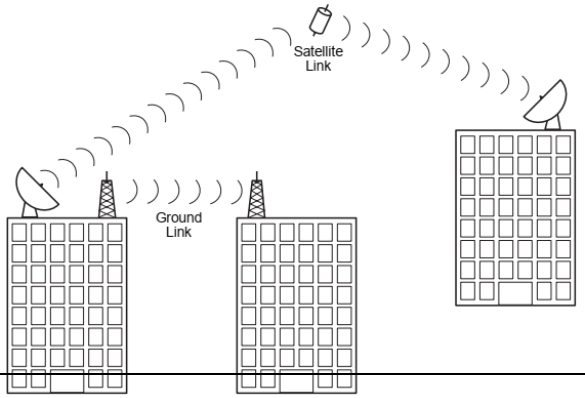
In narrow-band radio communications (also called single-frequencyradio), transmissions occur at a single radio frequency. The range ofnarrow-band radio is greater than that of infrared, effectivelyenabling mobile computing over a limited area. Neither the receivernor the transmitter must be placed along a direct line of sight; thesignal can bounce off walls, buildings, and even the atmosphere, butheavy walls, such as steel or concrete enclosures, can block the signal.

Spread-Spectrum Radio Transmission

Spread-spectrum radio transmission is a technique originally developed by the military to solve several communication problems.Spread-spectrum improves reliability, reduces sensitivity to interference and jamming, and is less vulnerable to eavesdropping thansingle-frequency radio. Spread-spectrum radio transmissions arecommonly used for WAN transmissions that connect multiple LANsor network segments together.As its name suggests, spread-spectrum transmission uses multiple frequencies to transmit messages. Two techniques employed are frequency hopping and direct sequence modulation.

Microwave

Microwave technology has applications in all three of the wirelessnetworking scenarios: LAN, extended LAN, and mobile networking. As shown in Figure, microwave communication can take two forms: terrestrial (ground) links and satellite links. The frequenciesand technologies employed by these two forms are similar, but distinct differences exist between them.Mobile computing is a growing technology that provides almostunlimited range for



traveling computers by using satellite and cellular phone networks to relay the signal to a home network. Mobilecomputing typically is used with portable PCs or personal digitalassistant (PDA) devices.Three forms of mobile computing are as follows:

- Packet-radio networking. The mobile device sends and receivesnetwork-style packets via satellite. Packets contain a source anddestination address, and only the destination device can receiveand read the packet.
- Cellular networking. The mobile device sends and receivescellular digital packet data (CDPD) using cellular phone technology and the cellular phone network. Cellular networkingprovides very fast communications.
- Satellite station networking. Satellite mobile networking stations use satellite microwave technology.

Bluetooth

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF (Ultra High Frequency) radio waves in the ISM band from 2.400 to 2.485 GHz from fixed and mobile devices, and building personal area networks (PANs). It was originally conceived as a wireless alternative to RS-232 data cables.

Bluetooth is managed by the Bluetooth Special Interest Group (SIG), which has more than 30,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics. The IEEE standardized Bluetooth as IEEE 802.15.1, but no longer maintains the standard. The Bluetooth SIG oversees development of the specification, manages the qualification program, and protects the trademarks.A manufacturer must meet Bluetooth SIG standards to market it as a Bluetooth device.A network of patents apply to the technology, which are licensed to individual qualifying devices.

The idea of this name was proposed in 1997 by Jim Kardach of Intel who developed a system that would allow mobile phones to communicate with computers.At the time of this proposal he was reading Frans G. Bengtsson's historical novel The Long Ships about Vikings and King Harald Bluetooth.

The Bluetooth logo is a bind rune merging the Younger Futhark runes Runic letter (ᚼ, Hagall) and Runic letter (ᛒ, Bjarkan), Harald's initials.

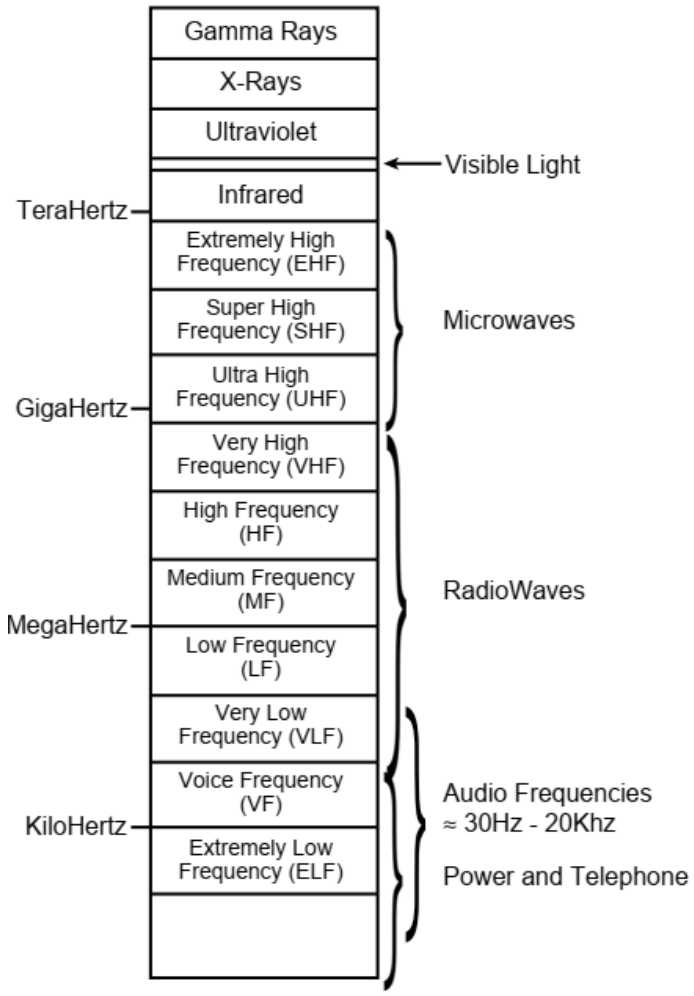
Ranges of Bluetooth devices by class

Class	Max. permitted power		Typ. range (m)
	(mW)	(dBm)	
1	100	20	~100
1.5 (BT 5 Vol 6 Part A Sect 3)	10	10	~20
2	2.5	4	~10
3	1	0	~1
4	0.5	−3	~0.5

COMPARISON OF CABLE MEDIA

Cable Type	*Cost*	*Installation*	*Capacity*	*Range*	*EMI*
Coaxial Thinnet	Less than STP	Inexpensive/easy	10Mbps typical	185 m	Less sensitive than UTP
Coaxial Thicknet	Greater than STP, less than fiber	Easy	10Mbps typical	500 m	Less sensitive than UTP
Shielded twisted-pair (STP)	Greater than UTP, less than Thicknet	Fairly easy	16Mbps typical up to 500Mbps	100 m typical	Less sensitive than UTP
Unshielded twisted-pair (UTP)	Lowest	Inexpensive/easy	10Mbps typical up to 100Mbps	100 m typical	Most sensitive
Fiber-optic	Highest	Expensive/difficult	100Mbps typical	10s of kilometers	Insensitive

2.1.3 Different Frequency Ranges



2.2 Multiplexing and Demultiplexing

Multiplexing and Demultiplexing services are provided in almost every protocol architecture ever designed. UDP and TCP perform the demultiplexing and multiplexing jobs by including two special fields in the segment headers: the source port number field and the destination port number field. Multiplexing: Gathering data from multiple application processes of sender, enveloping that data with header and sending them as a whole to the intended receiver is called as multiplexing. De-multiplexing: Delivering received segments at receiver side to the correct app layer processes is called as de-multiplexing.

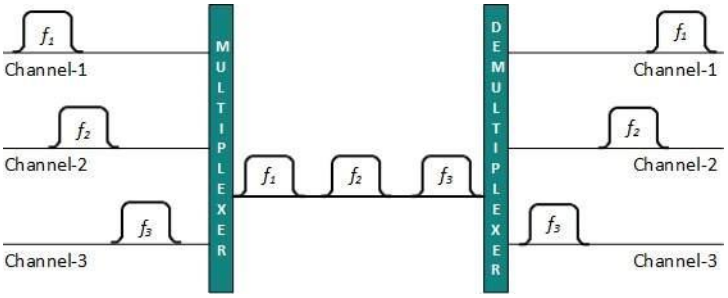
2.2.1 Multiplexing Type

Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams.

Communication is possible over the air (radio frequency), using a physical media (cable), and light (optical fiber). All mediums are capable of multiplexing. When multiple senders try to send over a single medium, a device called Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium, identifies each, and sends to different receivers.

FDM (Frequency Division Multiplexing)

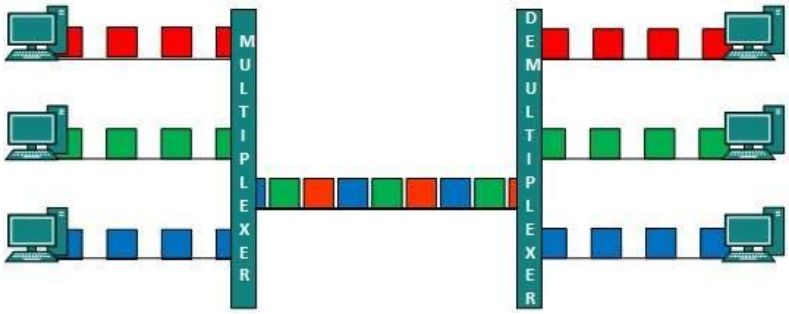
When the carrier is frequency, FDM is used. FDM is an analog technology. FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel. Each user can use the channel frequency independently and has exclusive access of it. All channels are divided in such a way that they do not overlap with each other. Channels are separated by guard bands. Guard band is a frequency which is not used by either channel.



TDM (Time Division Multiplexing)

TDM is applied primarily on digital signals but can be applied on analog signals as well. In TDM the shared channel is divided among its user by means of time slot. Each user can transmit data within the provided time slot only. Digital signals are divided in frames, equivalent to time slot i.e. frame of an optimal size which can be transmitted in given time slot.TDM works in synchronized mode. Both ends, i.e. Multiplexer and De-multiplexer are timely synchronized and both switch to next channel simultaneously.

When channel A transmits its frame at one end,the De-multiplexer provides media to channel A on the other end.As soon as the channel A's time slot expires, this side switches to channel B. On the other end, the De-multiplexer works in a synchronized manner and provides media to channel B. Signals from different channels travel the path in interleaved manner.



CDM (Code Division Multiplexing)

Multiple data signals can be transmitted over a single frequency by using Code Division Multiplexing. FDM divides the frequency in smaller channels but CDM allows its users to full bandwidth and transmit signals all the time using a unique code. CDM uses orthogonal codes to spread signals. Each station is assigned with a unique code, called chip. Signals travel with these codes independently, inside the whole bandwidth. The receiver knows in advance the chip code signal it has to receive.

WDM (Wavelength Division Multiplexing)

Light has different wavelength (colors). In fiber optic mode, multiple optical carrier signals are multiplexed into an optical fiber by using different wavelengths. This is an analog multiplexing technique and is done conceptually in the same manner as FDM but uses light as signals.Further, on each wavelength time division multiplexing can be incorporated to accommodate more data signals.

2.3 Switching Techniques

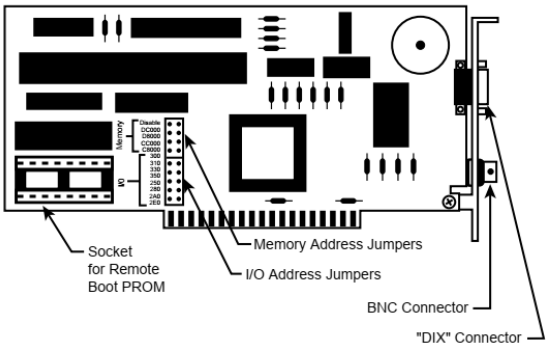
There three switching techniques are there: **(for more detail see OSI reference layers, Network layer's Packet Delivering techniques)**

- Circuit Switching
- Message Switching
- Packet Switching

2.4 Network Devices

2.4.1 Layer 1 Devices

LAN Card



When devices are attached to a network, some mechanism mustexist for transferring the information from one device to a transmission medium so that the other device or devices on the network canreceive the information. Likewise, the receiving device must alsohave some mechanism to receive this information from the transmission medium, so that it can process the information. This chapter, "Connectivity Devices and Transfer Mechanisms, "describe to you the function and workings of some of the commondevices used to attach components to the network's transmission medium. This chapter examines the role of the network adapter card, also known as a network interface card (NIC). Because a network adapter card is the most common mechanism for attaching PCs to anetwork, it is deserving of an entire chapter.

A network adapter card is a hardware device that installs in a PCand provides an interface from a PC to the transmission medium.Most PC networks, including ethernet, token-ring, and ARCNet, use network adapter cards. The network adapter card is thus anessential part of networking, and an understanding of network adapter cards is crucial for any networking professional.This chapter begins by explaining the mechanisms used to transfer data from the PC to the transmission medium. From there, configurable options on a network card are examined. That sectionexplains the different properties that are configurable on a network adapter card. The next section of the chapter goes on to explain the installation of a network adapter card, and the chapter concludeswith ways to resolve hardware conflicts. To communicate, the operating system and the network adaptermust agree on certain important parameters, called resource settings. Some common resource settings for a network adapter are as follows:

- IRQ(Interrupt Request Line)
- Base I/O port address

- Base memory address
- DMA channel (Direct Memory Access channel)
- Boot PROM
- MAC address
- Ring speed (token-ring cards)
- Connector type

Modem

Standard telephone lines can transmit only analog signals.Computers, however, store and transmit data digitally. Modems cantransmit digital computer signals over telephone lines by convertingthem to analog form.Converting one signal form to another (digital to analog in this case)is called modulation. Recovering the original signal is called demodulation. The word “modem” derives from the termsmodulation/demodulation.

Modems can be used to connect computer devices or entire networks that are at distant locations. (Before digital telephone linesexisted, modems were about the only way to link distant devices.)Some modems operate constantly over dedicated phone lines.Others use standard public switched-telephone network (PSTN)dial-up lines and make a connection only when one is required.

DSL & ADSL

Digital Subscriber Line (DSL) technology is a Copper Loop Transmission Technology, which satisfies bottleneck problems that are often associated with the last mile between the network and service providers.While DSL technology provides dramatic improvements in speed, (up to 8+ Mbps) compared to other network access methods, the true strength of DSL-based service opportunities lies in the actions like:

- Multimedia applications required by today's network users.
- Performance and reliability.
- Economics.

As shown in the following sample comparison chart, DSL-based services offer Performance Benefits for the Network Service Users when compared to other network access methods. In Addition, DSL-based services expand these operational improvements for public and private (Campus) operators.One of the compelling advantages of DSL technology is that it is the NSP and helps the Service Users to take full advantage of the existing infrastructure, layer two and layer three Protocols (such as Frame Relay, ATM and IP), and have reliable network services already entrusted to come.

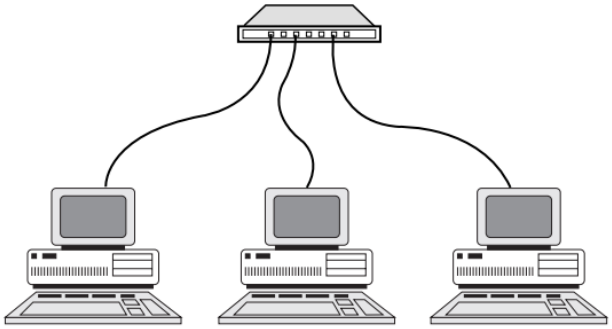
Asymmetric digital subscriber line (ADSL) is a type of digital subscriber line (DSL) technology, a data communications technology that enables faster data transmission over copper telephone lines than a conventional voiceband modem can provide. ADSL differs from the less common symmetric digital subscriber line (SDSL). In ADSL, bandwidth and bit rate are said to be asymmetric, meaning greater toward the customer premises (downstream) than the reverse (upstream). Providers usually market ADSL as a service for consumers for Internet access for primarily downloading content from the Internet, but not serving content accessed by others.

ADSL works by using the frequency spectrum above the band used by voice telephone calls.With a DSL filter, often called splitter, the frequency bands are isolated, permitting a single telephone line to be used for both ADSL service and telephone calls at the same time. ADSL is generally only installed for short distances from the telephone exchange (the last mile), typically less than 4 kilometres (2 mi),[2] but has been known to exceed 8 kilometres (5 mi) if the originally laid wire gauge allows for further[clarification needed] distribution.At the telephone exchange, the line generally terminates at a digital subscriber line access multiplexer (DSLAM) where another frequency splitter separates the voice band signal for the conventional phone network. Data carried by the ADSL are typically routed over the telephone company's data network and eventually reach a conventional Internet Protocol network.

Hub

Hubs, also called wiring concentrators, provide a central attachmentpoint for network cabling (see Figure). Hubs come in threetypes:

- Passive
- Active
- Switching (Smart/Intelligent Hub)



The following sections describe each of these types in more detail.

Passive Hubs

Passive hubs do not contain any electronic components and do notprocess the data signal in any way. The only purpose of a passivehub is to combine the signals from several network cable segments.All devices attached to a passive hub receive all the packets that passthrough the hub.Because the hub doesn't clean up or amplify the signals (in fact, thehub absorbs a small part of the signal), the distance between acomputer and the hub can be no more than half the maximum permissible distance between two computers on the network. For example, ifthe network design limits the distance between two computers to200 meters, the maximum distance between a computer and thehub is 100 meters.

Active Hubs

Active hubs incorporate electronic components that can amplify andclean up the electronic signals that flow between devices on the network. This process of cleaning up the signals is called signal regeneration. Signal regeneration has the following benefits:

- The network is more robust (less sensitive to errors).
- Distances between devices can be increased.

These advantages generally outweigh the fact that active hubs costconsiderably more than passive hubs.

Intelligent Hubs

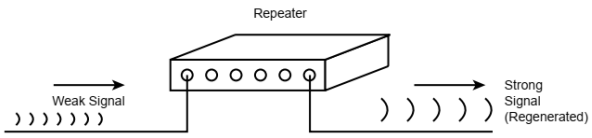
Intelligent hubs are enhanced active hubs. Several functions can addintelligence to a hub:

- Hub management. Hubs now support network management protocols that enable the hub to send packets to a central network console. These protocols also enable the console to control the hub; for example, a network administrator can order the hub to shut down a connection that is generating network errors.
- Switching. The latest development in hubs is the switching hub, which includes circuitry that very quickly routes signals between ports on the hub. Instead of repeating a packet to all ports on the hub, a switching hub repeats a packet only to the port that connects to the destination computer for the packet. Many switching hubs have the capability of switching packets to the fastest of several alternative paths. Switching hubs are replacing bridges and routers on many networks.

In essence, a switching hub acts like a very fast bridge, which is whatis described in the next section. Switching hubs are the most expensive of hubs on the market. Often they are simply referred to asSwitches. As for the exam, think of all types of hubs as simply a hub.

Repeater

As you learned in Chapter, "Transmission Media," all media attenuate the signals they carry. Each media type, therefore, has a maximum range that it can reliably carry data. The purpose of a repeateris to extend the maximum range for the network cabling.A repeater is a network device that repeats a signal from one portonto the other ports to which it is connected (see Figure).



Repeaters operate at the OSI Physical layer. (Refer to “The OSI Reference Model”.) A repeater does not filter or interpret—it merely repeats (regenerates) a signal, passing all network traffic in all directions. A repeater doesn’t require any addressing information from the data frame because a repeater merely repeats bits of data. This means that if data is corrupt, a repeater will regenerate the signal anyway. Repeater will even repeat a broadcast storm caused by a malfunctioning adapter. The advantages of repeaters are that they are inexpensive and simple. Also, although they cannot connect networks with dissimilar data

2.4.2 Layer 2 Devices

Switch

Switches occupy the same place in the network as hubs. Unlike hubs, switches examine each packet and process it accordingly rather than simply repeating the signal to all ports. Switches map the Ethernet addresses of the nodes residing on each network segment and then allow only the necessary traffic to pass through the switch. When a packet is received by the switch, the switch examines the destination and source hardware addresses and compares them to a table of network segments and addresses. If the segments are the same, the packet is dropped or “filtered”; if the segments are different, then the packet is “forwarded” to the proper segment. Additionally, switches prevent bad or misaligned packets from spreading by not forwarding them. Filtering packets and regenerating forwarded packets enables switching technology to split a network into separate collision domains. The regeneration of packets allows for greater distances and more nodes to be used in the total network design, and dramatically lowers the overall collision rates. In switched networks, each segment is an independent collision domain. This also allows for parallelism, meaning up to one-half of the computers connected to a switch can send data at the same time. In shared networks all nodes reside in a single shared collision domain.

Easy to install, most switches are self-learning. They determine the Ethernet addresses in use on each segment, building a table as packets are passed through the switch. This “plug and play” element makes switches an attractive alternative to hubs.

Managed Switch

Managed switches have more capability than unmanaged switches but also require a skilled administrator or engineer to make the most of them. A managed switch allows you have better control of your network and all the traffic moving through it. An unmanaged switch allows Ethernet devices to communicate with one another automatically using auto-negotiation to determine parameters such as the data rate and whether to use half-duplex or full-duplex mode.

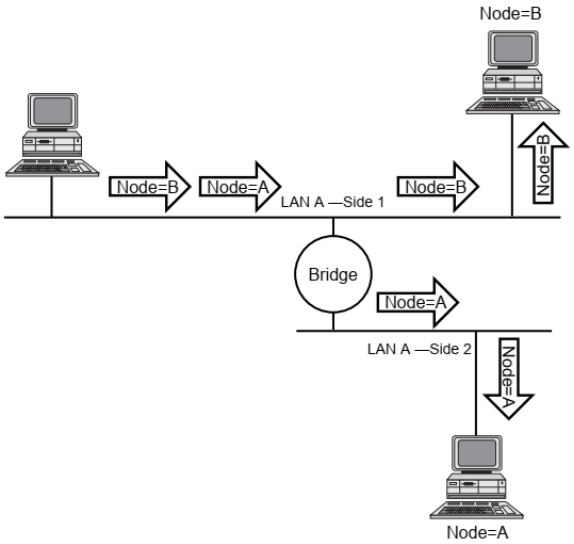
A managed switch lets you adjust each port on the switch to any setting you desire, allowing you to monitor and configure your network in many different ways. It also provides greater control over how data travels over the network and who has access to it. Managed switches generally offer SNMP (Simple Network Management Protocol), which allows you to monitor the status of connections and gives you statistics like traffic throughput, network errors and port status.

Unmanaged Switch

An Unmanaged Switch simply allows Ethernet devices to communicate with one another, such as a PC or network printer, and those are typically what we call plug and play. They are shipped with a fixed configuration and do not allow any changes to this configuration. An Unmanaged Switch is typically used in small networks or to add temporary workgroups to larger networks. The key difference between Managed and Unmanaged Switches is the ability to configure the Switch.

Bridge

Bridges, on the other hand, can extend the maximum size of a network. Although the bridged network in Figurelooks much likethe earlier example of a network with a repeater, the bridge is amuch more flexible device. Bridges operate at the MAC sublayer ofthe OSI Data Link layer.A repeater passes on all signals that it receives. A bridge, on theother hand, is more selective and passes only those signals targetedfor a computer on the other side. A bridge can make this determination because each device on the network is identified by a uniquephysical address.



Each packet that is transmitted bears the address of the device towhich it should be delivered. The process works as follows (refer toFigure):

1. The bridge receives every packet from either side of it on LAN A.
2. The bridge references an internal table of addresses. This table is either learned by the bridge, from previous packet deliveries on the network, or manually programmed into the bridge.
3. Packets on LAN A – Side 1 that are addressed to devices on LAN A – Side 1 and packets on LAN A – Side 2 that are addressed to devices on LAN A – Side 2, are not passed along to the other side by the bridge. These packets can be delivered without the help of the bridge.
4. Packets on LAN A – Side 1 addressed to devices on LAN A – Side 2 are retransmitted, by the bridge to LAN A – Side 2 for delivery. Similarly, the appropriate packets on LAN A – Side 2 are retransmitted to LAN A – Side 1.

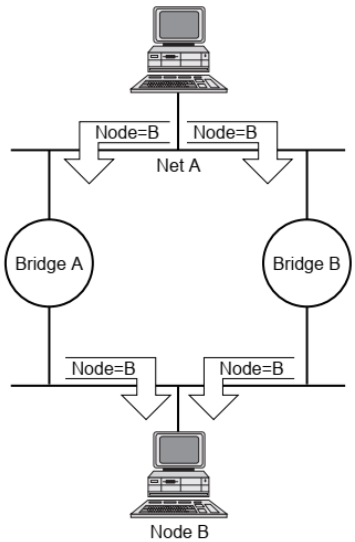
Bridges come in two main forms. One type of bridge is what isknown as a **transparent or learning bridge**. This type of bridge istransparent to the device sending the packet. At the same time thisbridge will learn over time what devices exist on each side of it. Thisis done by the bridge's ability to read the Data-Link information oneach packet going across the network. By analyzing these packets,and seeing the source MAC address of each device, the bridge is ableto build a table of which devices exist on what side of it. There usually is a mechanism for a person to go in and also program thebridge with address information as well. Learning bridges function asdescribed in step 2, automatically updating their address tables asdevices are added to or removed from the network. Ethernet networks almost always use a transparent bridge.

Another type of bridge is a **source routing bridge**. This type of bridgeis employed on a token-ring network. A source routing bridge is abridge that reads information appended to the packet by the sendingdevice. This additional information in the packet will state the routeto the destination segment on the network. A source routing bridgewill analyze this information to determine whether or not thisstream of data should or should not be passed along.

2.4.3 Layer 3 Devices

Router

Bridges are suitable for relatively simple networks, but bridges havecertain limitations that become more significant in complex networksituations. One limitation of bridges is that packets intended for allpeople on a subnet, also known as a broadcast, are received by everysingle device on the network. By being able to section off a LANsegment into different network segments, routers allow you to control and group devices that work together to be on the same networksegment.



Consider the network in Figure. Both bridges are aware of theexistence of

Node B, and both can pick up the packet from Net Aand forward it. At the very least, the same packet can arrive twice atNode B.A worse case, however, is that these relatively unintelligent bridgescan start passing packets around in loops, which results in an everincreasing number of packets that circulate on the network andnever reach their destinations. Ultimately, such activity can (andwill) saturate the network.An algorithm, called the spanning tree algorithm, enables complexEthernet networks to use bridges while redundant routes exist. Thealgorithm enables the bridges to communicate and construct a logical network without redundant paths. The logical network is reconfigured if one of the paths fails.

Routers organize the large network in terms of logical network segments. Each network segment is assigned an address so that everypacket has both a destination network address and a destinationdevice address.Routers are more “intelligent” than bridges. Not only do routersbuild tables of network locations, but they also use algorithms todetermine the most efficient path for sending a packet to any givennetwork. Even if a particular network segment isn’t directly attachedto the router, the router knows the best way to send a packet to adevice on that network. For example, Router Aknows that the most efficient step is to send the packet to Router C,not Router B.

Layer 3 Switch

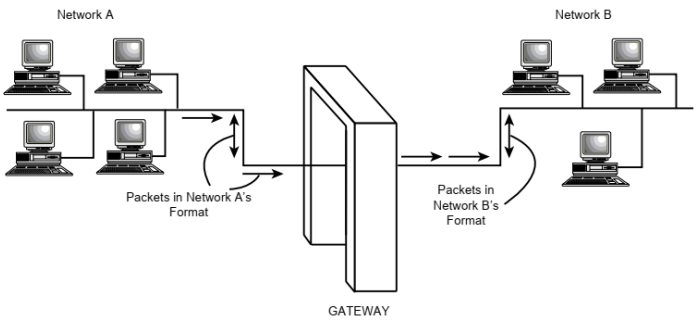
It acts as a switch because it connects devices that are on the same IP subnet or virtual LAN, and it performs at or near wire speed. But it also acts as a router because it has IP routing intelligence built in.Layer 3 switches are like a high-speed router without the WAN connectivity.

Before defining Layer 3 switches, let's understand what a regular switch and a router do.A switch works at Layer 2 of the OSI model -- the data-link layer. It is a LAN device that can also be called a multiport bridge. A switch forwards Ethernet frames between Ethernet devices. Switches do not care about IP addresses, nor do they even examine IP addresses as the frames flow through the switch. Instead, they forward frames based on the media access control (MAC) address.Every Ethernet device and port has its own unique 16-digit hexadecimal address. The switch maintains a database of MAC addresses and ports where the MAC addresses were last seen. This is known as a forwarding table. And unlike a network hub that simply duplicates data and broadcasts all frames out of every port, switches maintain their bridge forwarding tables, which makes the forwarding of frames far more efficient.

Brouters

A brouter is a router that also can act as a bridge. A brouterattempts to deliver packets based on network protocol information,but if a particular Network layer protocol isn’t supported, thebrouter bridges the packet using device addresses.

Gateway



The term “gateway” originally was used in the Internet protocolsuite to refer to a router. Today, the term “gateway” more commonlyrefers to a system functioning at the top levels of the OSI modelthat enables communication between dissimilar protocol systems. Agateway generally is dedicated to a specificconversion, and the exactfunctioning of the gateway depends on the protocol translations itmust perform. Gateways commonly function at the OSI Applicationlayer, but actually can operate at any level of the OSI model.

Gateways connect dissimilar environments by removing the layeredprotocol information of incoming packets and replacing it with thepacket information necessary for the dissimilar environment (see Figure).

2.4.4 Network Printer

A network printer is a printer that is accessible by network connection, making it usable by other computers connected to the network. The printer may have its own network connection, or use the network connection of a single dedicated computer to which it has a local connection.

A network printer is part of a workgroup or network of computers that can all access the same printers at the same time. A network printer does not have to have a physical connection to the network. Instead, it can also be connected wirelessly and assigned to a workgroup. Network printers efficiently meet the needs of multiple employees with a single printer. Network printers offer flexibility and efficiency to all employees in the office; they can operate with multiple platforms (Windows, Mac, Linux, etc.) and a variety of different printer types (laser, inkjet, thermal, etc.). This means users throughout the office can access network printers regardless of the platform in use on their device. Additionally, network printing solutions offer employees a variety of print options when various types of printers are connected to the network.As a downside, with multiple users capable of accessing the same printers, projects can be delayed when the printer is already in use. Additionally, if the network goes down then printers become inaccessible.

2.4.5 Wireless Network Devices

Wireless Router

A wireless router is a device that performs the functions of a router and also includes the functions of a wireless access point. It is used to provide access to the Internet or a private computer network. Depending on the manufacturer and model, it can function in a wired local area network, in a wireless-only LAN, or in a mixed wired and wireless network.

Access Point (AP)

In computer networking, a wireless access point (WAP), or more generally just access point (AP), is a networking hardware device that allows a Wi-Fi device to connect to a wired network. The AP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself. An AP is differentiated from a hotspot, which is the physical location where Wi-Fi access to a WLAN is available.

An AP connects directly to a wired local area network, typically Ethernet, and the AP then provides wireless connections using wireless LAN technology, typically Wi-Fi, for other devices to use that wired connection. APs support the connection of multiple wireless devices through their one wired connection.

Unit-3

Network Protocols, Network Routing

3.1 Packets and Protocols

The purpose of a network is to exchange information among computers, and protocols are the rules by which computers communicate. Computers, like humans, can adopt any number of systems forpassing messages, as long as the sending and receiving computers areusing the same (or compatible) rules. Computers, therefore, mustagree on common protocols before they can communicate. Failing todo so would create a bewildering situation similar to what you'd faceif you read a book in Russian to a listener who speaks onlyCherokee.You can classify the many tasks that network protocols must overseeinto a few basic categories. Think of these categories chronologically,as a series of steps (each step including a collection of related tasks)that must take place before the data can reach the transmissionmedium. These steps are the layers of a protocol stack, as described earlier. In one sense, the term layer is more than metaphorical.Each layer of the stack (the Application layer, the Presentation layer,and so on) adds a layer of information to the packet; the corresponding layer of the receiving computer needs to process the incomingpacket.The purpose of the layering structure is to enable vendors to adaptto specific hardware and software components without having torecreate the entire protocol stack.

Protocols describe the way in which network data is encapsulated inpackets on the source end, sent via the network to a destination, andthen reconstructed at the destination into the appropriate file,instruction, or request. Breaking network data into packet-sizedchunks provides smoother throughput because the small packetsdon't tie up the transmission medium as a larger unit of data might.Also, packets simplify the task of error detection and correction.Each file is checked separately for errors, and if an error is discovered, only that packet (rather than a whole file) must be retransmitted.The exact composition of a network packet depends on the protocols you're using. In general, network packets contain the following:

- Header. The header signifies the start of the packet and contains a bundle of important parameters, such as the source and destination address and time/synchronization information.
- Data. This portion of the packet contains the original data being transmitted.
- Trailer. The trailer marks the end of the packet and typically contains error-checking (Cyclical Redundancy Check, or CRC) information.

3.2 TCP/IP Stack

The TCP/IP protocol suite (also commonly called the Internet protocol suite) was originally developed by the United States Department of Defence (DoD) to provide robust service on large internetworks that incorporate a variety of computer types. Part of the mainpurpose of this protocol was for it to be hardware-independent. Insome literature, the TCP/IP protocol suite is referred to as the DoDmodel. In recent years, the Internet protocols constitute the mostpopular network protocols currently in use.One reason for the popularity of TCP/IP is that no one vendorowns it, unlike the IPX/SPX, DNA, SNA, or AppleTalk protocolsuites, all of which are controlled by specific companies. TCP/IPevolved in response to input from a wide variety of industry sources.Consequently, TCP/IP is the most open of the protocol suites and issupported by the widest variety of vendors. Virtually every brand ofcomputing equipment now supports TCP/IP. This has led to someproblems, though. Because TCP/IP is an open standard, sometimesone vendor's implementation of TCP/IP does not work with another's implementation.

3.2.1 Internet Protocol (IP)

The Internet Protocol (IP) is a connectionless protocol that providesdatagram service, and IP packets are most commonly referred to asIP datagrams. IP is a packet-switching protocol that performs theaddressing and route selection. An IP header is appended to packets,which are transmitted as frames by lower-level protocols. IP routespackets through internetworks by utilizing routing tables that arereferenced at each hop. Routing determinations are made by consulting logical and physical network device information, as providedby the Address Resolution Protocol (ARP).IP performs packet disassembly and reassembly as required by packet size limitations defined for the Data Link and Physical layersbeing implemented. IP also performs error checking on the headerdata using a checksum, although data from upper layers is not errorchecked.

3.2.2 Connection Oriented Protocol (TCP)

The Transmission Control Protocol (TCP) is an internetworkconnection-oriented protocol that corresponds to the OSI Transportlayer. TCP provides full-duplex, end-to-end connections. When theoverhead of end-to-end communication acknowledgment isn'trequired, the User Datagram Protocol (UDP) can be substituted forTCP at the Transport (host-to-host) level. TCP and UDP operate atthe same layer.

TCP corresponds to SPX in the NetWare environment (see the"NetWare IPX/SPX" section). TCP maintains a logical connectionbetween the sending and receiving computer systems. In this way,the integrity of the transmission is maintained. TCP detects anyproblems in the transmission quickly and takes action to correctthem. The trade-off is that TCP isn't as fast as UDP, due to thenumber of acknowledgments received by the sending host.TCP also provides and assumes message fragmentation and reassembly and can accept messages of any length from upper-layer protocols. TCP fragments message streams into segments that can behandled by IP. This process enables the application being used to notbreak up the data into smaller blocks. IP still can perform fragmentation for UDP packets and further fragmentation for TCP packets.When used with IP, TCP adds connection-oriented service and performs segment synchronization, adding sequence numbers at thebyte level.In addition to message fragmentation, TCP can multiplex conversations with upper-layer protocols and can improve use of networkbandwidth by combining multiple messages into the same segment.Each virtual-circuit connection is assigned a connection identifiercalled a port, which identifies the datagrams associated with thatconnection.

3.2.3 Connectionless Protocol (UDP)

The User Datagram Protocol (UDP) is a connectionless Transport(host-to-host) layer protocol. UDP does not provide messageacknowledgments; rather, it simply transports datagrams.Like TCP, UDP utilizes port addresses to deliver datagrams. Theseport addresses, however, aren't associated with virtual circuits andmerely identify local host processes. UDP is preferred over TCPwhen high performance or low network overhead is more criticalthan reliable delivery. Because UDP doesn't need to establish,maintain, and close connections, or control data flow, it generallyoutperforms TCP. The downfall in UDP is that it does not performas reliably as TCP when transmitting data; thus, UDP is often usedwhen transmitting smaller amounts of data.

UDP is the Transport layer protocol used with the Simple NetworkManagement Protocol (SNMP), the standard network managementprotocol used with TCP/IP networks. UDP enables SNMP to provide network management with a minimum of network overhead.

3.2.4 HTTP

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems.[1] HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen. HTTP was developed to facilitate hypertext and the World Wide Web.HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it. This is the main reason that it is difficult to implement Web sites that react intelligently to user input. This shortcoming of HTTP is being addressed in a number of new technologies, including ActiveX, Java, JavaScript and cookies.

3.2.5 FTP

The File Transfer Protocol (FTP) is a protocol for sharing filesbetween networked hosts. FTP enables users to log on to remotehosts. Logged-on users can inspect directories, manipulate files, execute commands, and perform other commands on the host. FTPalso has the capability of transferring files between dissimilar hostsby supporting a file request structure that is independent of specificoperating systems.

3.2.6 SMTP

The Simple Mail Transfer Protocol (SMTP) is a protocol for routingmail through internetworks. SMTP uses the TCP and IP protocols.SNMP doesn't provide a mail interface for the user. Creation, management, and delivery of messages to end users must be performedby an email application.

3.2.7 POP3

Post Office Protocol (POP) is an application-layer Internet standard protocol used by e-mail clients to retrieve e-mail from a mail server. POP version 3 (POP3) is the version in common use.POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail, probably using POP3. This standard protocol is built into most popular e-mail products, such as Eudora and Outlook Express. It's also built into the Netscape and Microsoft Internet Explorer browsers.An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

3.2.8 Simple Mail Transfer Protocol (SMTP)

The Simple Mail Transfer Protocol (SMTP) is a protocol for routingmail through internetworks. SMTP uses the TCP and IP protocols.SNMP doesn't provide a mail interface for the user. Creation, management, and delivery of messages to end users must be performedby an email application

3.2.9 Remote Terminal Emulation (TELNET)

TELNET is a terminal emulation protocol. TELNET enables PCsand workstations to function as dumb terminals in sessions withhosts on internetworks. TELNET implementations are available formost end-user platforms, including UNIX (of course), DOS,Windows, and Macintosh OS.

3.2.10 ARP

Three types of address information are used on TCP/IP internetworks:

- Physical addresses. Used by the Data Link and Physical layers.
- IP addresses. Provide logical network and host IDs. IP addresses consist of four numbers typically expressed in dotted-decimal form.
- Logical node names. Identify specific hosts with alphanumeric identifiers, which are easier for users to recall than the numeric IP addresses. An example of a logical node name is MYHOST.COM.

Given an IP address, the Address Resolution Protocol (ARP) candetermine the physical address used by the device containing the IPaddress. ARP maintains tables of address resolution data and canbroadcast packets to discover addresses on the network segment oruse previously cached entries. The physical addresses discovered byARP can be provided to Data Link layer protocols. All addresses inthe ARP table are only local addresses. Any non-local address contains the hardware address of the local port on the router that isused to access that non-local segment.

3.3 IPX/SPX

The following subsections deal with protocols in the IPX/SPX protocol suite that relate back to the Network and Transport layers ofthe OSI model.

3.3.1 IPX

The Internetwork Packet Exchange Protocol (IPX) is a Network layerprotocol that provides connectionless (datagram) service. (IPX wasdeveloped from the XNS protocol originated by Xerox.) As aNetwork layer protocol, IPX is responsible for internetwork routingand for maintaining network logical addresses. Routing uses the RIPprotocol (described later in this section) to make route selections.IPX provides similar functionality as UDP does in the TCP/IP protocol suite.IPX relies on hardware physical addresses found at lower layers toprovide network device addressing. IPX also uses sockets, or upperlayer service addresses, to deliver packets to their ultimate destinations. On the client, IPX support is provided as a component of theolder DOS shell and the current DOS NetWare requester. Windows3.1 utilizes the DOS shell client,

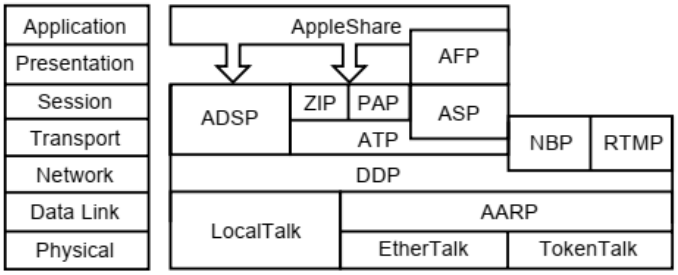
whereas Windows 95 andWindows NT supports IPX if you install a Novell-supplied client.Microsoft-supplied clients use the NWLink transport protocol supplied by Microsoft.

3.3.2 SPX

Sequenced Packet Exchange (SPX) is a Transport layer protocol thatextends IPX to provide connection-oriented service with reliabledelivery. Reliable delivery is ensured by the re-transmittal of packetsin the event of an error. SPX is derived from a similar SPX protocolin the XNS network protocol suite.SPX establishes virtual circuits called connections. The connection IDfor each connection appears in the SPX header. A given upper-layerprocess can be associated with multiple-connection IDs.

SPX is used in situations where reliable transmission of data is needed. SPX sequences the packets of data. Missing packets or packetsthat don't arrive in the order in which they were sent are detectedimmediately. In addition, SPX offers connection multiplexing,which is used in the printing environment. Many accounting programs, for example, call upon the services of SPX to ensure that datais sent accurately. On the client, SPX support is provided as a component of the older DOS shell and of the current NetWarerequester. SPX provides functionality similar to that of TCP in theTCP/IP protocol suite.As a network administrator, you do not often get to pick whetheryou wish to use IPX or SPX. It is often the applications one usesthat are pre-programmed to use one or the other. For example, inmost Novell networks, all file transfers are done using IPX. In thecase of printing, SPX is the protocol used.

3.4 AppleTalk



AppleTalk is the computing architecture developed by AppleComputer for the Macintosh family of personal computers.Although AppleTalk originally supported only Apple's proprietaryLocalTalk cabling system, the suite has been expanded to incorporate both ethernet and token-ring Physical layers. Within Microsoftoperating systems, AppleTalk is only supported by Windows NTServer. Windows NT Workstation and Windows 95 do not supportAppleTalk. AppleTalk cannot be used for Microsoft-to-Microsoftoperating system communication. It can be used only throughWindows NT servers supporting Apple clients.

AppleTalk originally supported networks of limited scope. TheAppleTalk Phase II specification issued in 1989, however, extendedthe scope of AppleTalk to enterprise networks. The Phase II specification also enabled AppleTalk to coexist on networks with other protocol suites. Figure presents a layered perspective of theAppleTalk protocols.

The LocalTalk, EtherTalk, and TokenTalk Link Access Protocols(LLAP, ELAP, and TLAP) integrate AppleTalk upper-layer protocolswith the LocalTalk, ethernet, and token-ring environments.Apple's Datagram Deliver Protocol (DDP) is a Network layer protocolthat provides connectionless service between two sockets. A socket isthe AppleTalk term for a service address. A combination of a deviceaddress, network address, and socket uniquely identifies eachprocess.

DDP performs network routing and consults routing tables maintained by Routing Table Maintenance Protocol (RTMP) to determine routing. Packet delivery is performed by the data link protocoloperating on a given destination network.The AppleTalk Transaction Protocol (ATP) is a connectionlessTransport layer protocol. Reliable service is provided through a system of acknowledgments and retransmissions. Retransmissions areinitiated automatically if an acknowledgment is not received within aspecified time interval. ATP reliability is based on transactions. Atransaction consists of a request followed by a reply. ATP is responsible for segment development and performs fragmentation andreassembly of packets that exceed the specifications for lower-layerprotocols. Packets include sequence numbers that enable messagereassembly and retransmission of lost packets. Only damaged or lostpackets are retransmitted.

The AppleTalk File Protocol (AFP) provides file services and isresponsible for translating local file service requests into formatsrequired for network file services. AFP directly translates commandsyntax and enables applications to perform file format translations.AFP is responsible for file system security, and verifies and encryptslogon names and passwords during connection setup.

3.5 NetBIOS name Protocol

NetBIOS is an interface that provides NetBIOS-based applicationswith access to network resources. Every computer on a WindowsNT network must have a unique name for it to be accessiblethrough the NetBIOS interface. This unique name is called a computer name or a NetBIOS name.

NetBIOS (Network Basic Input/Output System) is an applicationinterface that provides PC-based applications with uniform access tolower protocol layers. NetBIOS was once most closely associatedwith the NetBEUI protocol—NetBEUI, in fact, is an abbreviationfor NetBIOS Extended User Interface. In recent years, however,other vendors have recognized the importance of providing compatibility with PC-based applications through NetBIOS, and NetBIOSis now available with many protocol configurations. For instance,such terms as “NetBIOS over IPX” or “NetBIOS over TCP/IP” referto the protocols used with NetBIOS.All of Microsoft’s networking architecture references NetBIOSnames, thus it can be said that Microsoft Networking uses aNetBIOS interface to access components on the network.

3.6 L2CAP, RFCOMM Protocol

3.6.1 L2CAP (Logical Link Control and Adaption Protocol/Layer 2 Control Protocol)

This is layered over Baseband protocol and resides in the data link layer. The L2CAP is the big picture brains of a Bluetooth system. It manages the high level aspects of each connection (who is connected to who, whether to use encryption or not, what level of performance is required, etc.). In addition, it is responsible for converting the format of data as necessary between the APIs and the lower level Bluetooth protocols. The L2CAP is implemented in software and can execute either on the host system processor or on a local processor in the Bluetooth system. L2CAP provides connection oriented and connectionless data services to upper layer protocols with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions. L2CAP permits higher-level protocols and applications to transmit and receive L2CAP data packets up to 64 KB in length. Two link types are supported for Baseband layer: synchronous connection-oriented (SCO) links and asynchronous connection-less (ACL) links. SCO links support real-time voice traffics using reserved bandwidth. ACL links support best effort traffic. The L2CAP specification is defined for only ACL links and no support for SCO links is planned.

3.6.2 RFCOMM

RFCOMM (Radio Frequency Communication) is a simple transport protocol, which provides emulation of RS232 serial ports over the L2CAP protocol.The protocol is based on the ETSI standard TS 07.10. Only a subset of the TS 07.10 standard is used and an RFCOMM - specific extension is added, in the form of a mandatory credit based flow control scheme.The RFCOMM protocol supports up to 60 simultaneous connections between two BT devices. The number of connections that can be used simultaneously in a BT device is implementation-specific. For the purposes of RFCOMM, a complete communication path involves two applications running on different devices (the communication endpoints) with a communication segment between them.Basically two device types exist that RFCOMM must accommodate.Type 1 Devices are communication end points such as computers and printers.Type 2 Devices are those that are part of the communication segment; e.g. modems.

Though RFCOMM does not make a distinction between these two device types in the protocol, accommodating both types of devices impacts the RFCOMM protocol.The information transferred between two RFCOMM entities has been defined to support both type 1 and type 2 devices. Some information is only needed by type 2 devices while other information is intended to be used by both. In the

protocol, no distinction is made between type 1 and type 2. Since the device is not aware of the type of the other device in the communication path, each must pass on all available information specified by the protocol.

3.7 What is Routing?

Routing refers to establishing the routes that data packets take on their way to a particular destination. This term can be applied to data traveling on the Internet, over 3G or 4G networks, or over similar networks used for telecom and other digital communications setups. Routing can also take place within proprietary networks.

3.7.1 Requirements of Routing

In general, routing involves the network topology, or the setup of hardware, that can effectively relay data. Standard protocols help to identify the best routes for data and to ensure quality transmission. Individual pieces of hardware such as routers are referred to as "nodes" in the network. Different algorithms and protocols can be used to figure out how to best route data packets, and which nodes should be used. For example, some data packets travel according to a distance vector model that primarily uses distance as a factor, whereas others use Link-State Protocol, which involves other aspects of a "best path" for data.

Data packets are also made to give networks information. Headers on packets provide details about origin and destination. Standards for data packets allow for conventional design, which can help with future routing methodologies. As the world of digital technology evolves, routing will also evolve according to the needs and utility of a particular network.

3.7.2 Types of Routing

Routing is a process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another.There are 3 types of routing:

Static routing

Static routing is a process in which we have to manually add routes in routing table.

Advantages:–

- No routing overhead for router CPU which means a cheaper router can be used to do routing.
- It adds security because only administrator can allow routing to particular networks only.
- No bandwidth usage between routers.

Disadvantage:–

- For a large network, it is a hectic task for administrator to manually add each route for the network in the routing table on each router.
- The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have very good knowledge of the routes of the topology.

Dynamic Routing

Dynamic routing makes automatic adjustment of the routes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations and the routes to reach it. RIP and OSPF are the best examples of dynamic routing protocol. Automatic adjustment will be made to reach the network destination if one route goes down.A dynamic protocol have following features:

1. The routers should have the same dynamic protocol running in order to exchange routes.
2. When a router finds a change in the topology then router advertises it to all other routers.

Advantages:–

- Easy to configure.
- More effective at selecting the best route to a destination remote network and also for discovering remote network.

Disadvantage:–

- Consumes more bandwidth for communicating with other neighbours.
- Less secure than static routing.

Default Routing

This is the method where the router is configured to send all packets towards a single router (next hop). It doesn't matter to which network the packet belongs, it is forwarded out to router which is configured for default routing. It is generally used with stub routers. A stub router is a router which has only one route to reach all other networks.Using the same topology which we have used for the static routing before.

3.7.3 Routing Protocol

A routing protocol uses software and routing algorithms to determine optimal network data transfer and communication paths between network nodes. Routing protocols facilitate router communication and overall network topology understanding.A routing protocol is also known as a routing policy.

3.7.3.1 Exterior Routing Protocol

Border Gateway Protocol (BGP) v4: This provides public Internet routing protocol through exterior gateway routing. To get from place to place outside your network(s), i.e. on the Internet, you must use an Exterior Gateway Protocol. Exterior Gateway Protocols handle routing outside an Autonomous System and get you from your network, through your Internet provider's network and onto any other network. BGP is used by companies with more than one Internet provider to allow them to have redundancy and load balancing of their data transported to and from the Internet.Examples of an EGP:Border Gateway Protocol (BGP), and Exterior Gateway Protocol (Replaced by BGP).

BGP

Border Gateway Protocol (BGP) is a routing protocol used on the edge of autonomous systems (AS). It is an exterior routing protocol and calculates loop-free paths across the Internet. It is considered to use a path-vector routing algorithm. This means it tracks the path in terms of which AS it passes through, and does NOT track the 'route' through individual routers within an AS, and is not specifically capable of performing load balancing or packet forwarding itself. BGP is the routing protocol of choice and is used by all the Network Service Providers (NSPs) such as UUNet, Sprint, Cable & Wireless, Level3, Qwest etc. It is dynamic and handles outages and link failures fairly gracefully. To use BGP, you must have a router that supports BGP; register an AS Number and contact your provider to set up a BGP session. See the requirements page for more information.BGP has gone through three revisions. The current version in use is BGP4 and is supported by most router manufacturers including Cisco, Lucent/Bay, Juniper and many others, as well as by Unix and Linux programs such as Zebra.

3.7.3.2 Interior Routing Protocol

There are two types of Interior Routing Protocols namely Distance Vector Routing, and Link State Routing mentioned below:

Distance Vector Routing

These protocols selects best path in the basis of hop counts to reach a destination network in the particular direction. Dynamic protocol like RIP is an example of distance vector routing protocol. Hop count is each router which occurs in between the source and the destination network. The path with the least hop count will be chosen as the best path.

Advantages:–

- Updates of network are exchanged periodically.
- Updates (routing information) is always broadcast.
- Full routing tables are sent in updates.
- Routers always trust on routing information received from neighbor routers. This is also known as routing on rumours.

Disadvantages:–

- As the routing information are exchanged periodically, unnecessary traffic is generated which consumes available bandwidth.
- As full routing tables are exchanged, therefore it has security issues. If an authorized person enters the network, then the whole topology will be very easy to understand.
- Also broadcasting of network periodically creates unnecessary traffic.

RIP

The Routing Information Protocol (RIP) in the TCP/IP suite is notthe same protocol as RIP in the NetWare suite, although the twoserve similar functions. Internet RIP performs route discovery byusing a distance-vector method, calculating the number of hops thatmust be crossed to route a packet by a particular path. Although it works well in localized networks, RIP presents many weaknesses that limit its utility on wide-area internetworks. RIP's distancevector route discovery method, for example, requires more broadcasts and thus causes more network traffic than some other methods.The entire route table is also sent out on the broadcast, causing largeamounts of traffic as route tables become large. The Open ShortestPath First (OSPF) protocol, which uses the link-state route discoverymethod, is gradually replacing RIP.

IGRP

Interior Gateway Routing Protocol (IGRP) is a proprietary distance vector routing protocol used to communicate routing information within a host network. It was invented by Cisco.IGRP manages the flow of routing information within connected routers in the host network or autonomous system. The protocol ensures that every router has routing tables updated with the best available path. IGRP also avoids routing loops by updating itself with the changes occurring over the network and by error management.

Cisco created Interior Gateway Routing Protocol (IGRP) in response to the limitations in Routing Information Protocol (RIP), which handles a maximum hop count of 15. IGRP supports a maximum hop count of up to 255. The primary two purposes of IGRP are to:

- Communicate routing information to all connected routers within its boundary or autonomous system
- Continue updating whenever there is a topological, network or path change that occurs

IGRP sends a notification of any new changes, and information about its status, to its neighbours every 90 seconds.IGRP manages a routing table with the most optimal path to respective nodes and to networks within the parent network. Because it is a distance vector protocol, IGRP uses several parameters to calculate the metric for the best path to a specific destination. These parameters include delay, bandwidth, reliability, load and maximum transmission unit (MTU).

EIGRP

It is also known as hybrid routing protocol which uses the concept of both distance vector and link state routing protocol. Enhanced Interior Gateway Routing Protocol (EIGRP) is an example of this class if routing protocol. EIGRP acts as a link state routing protocol as it uses the concept of Hello protocol for neighbour discovery and forming adjacency. Also, partial updates are triggered when a change occurs. EIGRP acts as distance vector routing protocol as it learned routes from directly connected neighbours.

Link State Routing

Link State Routing Protocol – These protocols know more about the Internetwork than any other distancevector routing protocol. These re also known as SPF (Shortest Path First) protocol. OSPF is an example of link state routing protocol.

Advantages:–

- Hello messages, also known as keep-alive messages are used for neighbour discovery and recovery.

- Concept of triggered updates are used i.e. updates are triggered only when there is a topology change.
- Only that much updates are exchanged which is requested by the neighbour router.

Link state routing protocol maintains three tables namely:

- **Neighbour table**- the table which contains information about the neighbours of the router only, i.e., to which adjacency has been formed.
- **Topology table**- This table contains information about the whole topology i.e. contains both best and backup routes to particular advertised network.
- **Routing table**- This table contains all the best routes to the advertised network.

Advantages:–

- As it maintains separate tables for both best route and the backup routes (whole topology) therefore it has more knowledge of the inter network than any other distance vector routing protocol.
- Concept of triggered updates are used therefore no more unnecessary bandwidth consumption is seen like in distance vector routing protocol.
- Partial updates are triggered when there is a topology change, not a full update like distance vector routing protocol where whole routing table is exchanged.

OSPF

Open Shortest Path First (OSPF) is a link state routing protocol which was first defined as version 2 in RFC 2328. It is used to allow routers to dynamically learn routes from other routers and to advertise routes to other routers. Advertisements containing routes are referred to as Link State Advertisements (LSAs) in OSPF. OSPF router keeps track of the state of all the various network connections (links) between itself and a network it is trying to send data to. This makes it a link-state routing protocol. OSPF supports the use of classless IP address ranges and is very efficient. OSPF uses areas to organize a network into a hierarchal structure; it summarizes route information to reduce the number of advertised routes and thereby reduce network load and uses a designated router (elected via a process that is part of OSPF) to reduce the quantity and frequency of Link State Advertisements. OSPF does require the router have a more powerful processor and more memory than other routing protocols.

OSPF selects the best routes by finding the lowest cost paths to a destination. All router interfaces (links) are given a cost. The cost of a route is equal to the sum of all the costs configured on all the outbound links between the router and the destination network, plus the cost configured on the interface that OSPF received the Link State Advertisement on.

ISIS

IS-IS (pronounced eye-ess-eye-ess) is defined in ISO 10589. IS-IS is the descendant of the older OSI CLNS routing protocol. IS-IS is a dynamic, link state routing protocol. In an IS-IS network, there are End Systems, Intermediate Systems, Areas and Domains. End systems are user devices. Intermediate systems are routers. Routers are organized into local groups called 'areas' and several areas are grouped together into a 'domain'. IS-IS places Area routers into Layer 1, and routers that interconnect the Areas into Layer 2. IS-IS uses its own addressing scheme.There are two types of IS-IS addresses:

1. Network Service Access Point (NSAP): NSAP addresses identify network layer services, one for each service running.
2. Network Entity Title (NET): NET addresses identifynetwork layer entities or processes instead of services.

Devices may have more than one of each of the two types of addresses. However NET's should be unique, and the System ID portion of the NSAP must be unique for each system.

Unit-4

IP Addressing, Windows Server 2008

4.1 What is IP address?

An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number. However, because of the growth of the Internet and the depletion of available IPv4 addresses, a new version of IP (IPv6), using 128 bits for the IP address, was developed in 1995, and standardized in December 1998. In July 2017, a final definition of the protocol was published. IPv6 deployment has been ongoing since the mid-2000s.

IP addresses are usually written and displayed in human-readable notations, such as 172.16.254.1 in IPv4, and 2001:db8:0:1234:0:567:8:1 in IPv6. The size of the routing prefix of the address is designated in CIDR notation by suffixing the address with the number of significant bits, e.g., 192.168.1.15/24, which is equivalent to the historically used subnet mask 255.255.255.0. The IP address space is managed globally by the Internet Assigned Numbers Authority (IANA), and by five regional Internet registries (RIRs) responsible in their designated territories for assignment to end users and local Internet registries, such as Internet service providers. IPv4 addresses have been distributed by IANA to the RIRs in blocks of approximately 16.8 million addresses each. Each ISP or private network administrator assigns an IP address to each device connected to its network. Such assignments may be on a static (fixed or permanent) or dynamic basis, depending on its software and practices.

An IP address serves two principal functions. It identifies the host, or more specifically its network interface, and it provides the location of the host in the network, and thus the capability of establishing a path to that host. Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there." The header of each IP packet contains the IP address of the sending host, and that of the destination host.

4.2 Type of IP Address

4.2.1 IPv4

Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides the logical connection between network devices by providing identification for each device. There are many ways to configure IPv4 with all kinds of devices – including manual and automatic configurations – depending on the network type. IPv4 is based on the best-effort model. This model guarantees neither delivery nor avoidance of duplicate delivery; these aspects are handled by the upper layer transport.

An IPv4 address has a size of 32 bits, which limits the address space to 4294967296 (232) addresses. Of this number, some addresses are reserved for special purposes such as private networks (~18 million addresses) and multicast addressing (~270 million addresses). IPv4 addresses are usually represented in dot-decimal notation, consisting of four decimal numbers, each ranging from 0 to 255, separated by dots, e.g., 172.16.254.1. Each part represents a group of 8 bits (an octet) of the address. In some cases of technical writing, IPv4 addresses may be presented in various hexadecimal, octal, or binary representations.

Class structure

Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Number of addresses per network	Start address	End address
A	0	8	24	128 (2^7)	16777216 (2^{24})	0.0.0.0	127.255.255.255
B	10	16	16	16384 (2^{14})	65536 (2^{16})	128.0.0.0	191.255.255.255
C	110	24	8	2097152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255

Subnetting

In the early stages of development of the Internet Protocol, the network number was always the highest order octet (most significant eight bits). Because this method allowed for only 256 networks, it soon proved inadequate as additional networks developed that were independent of the existing networks already designated by a network number. In 1981, the addressing specification was revised with the introduction of classful network architecture.

Classful network design allowed for a larger number of individual network assignments and fine-grained subnetwork design. The first three bits of the most significant octet of an IP address were defined as the class of the address. Three classes (A, B, and C) were defined for universal unicast addressing. Depending on the class derived, the network identification was based on octet boundary segments of the entire address. Each class used successively additional octets in the network identifier, thus reducing the possible number of hosts in the higher order classes (B and C). The following table gives an overview of this now obsolete system.

Supernetting

Supernetting is the opposite of Subnetting. In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet. Supernetting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks. This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols.

- When multiple networks are combined to form a bigger network, it is termed as super-netting
- Super netting is used in route aggregation to reduce the size of routing tables and routing table updates

There are some points which should be kept in mind while supernetting:

1. All the IP address should be contiguous.
2. Size of all the small networks should be equal and must be in form of 2n.
3. First IP address should be exactly divisible by whole size of supernet.

4.2.2 IPv6

Internet Protocol version 6 is a new addressing protocol designed to incorporate all the possible requirements of future Internet known to us as Internet version 2. This protocol as its predecessor IPv4, works on the Network Layer (Layer-3). Along with its offering of an enormous amount of logical address space, this protocol has ample features to which address the shortcoming of IPv4.

So far, IPv4 has proven itself as a robust routable addressing protocol and has served us for decades on its best-effort-delivery mechanism. It was designed in the early 80's and did not get any major change afterward. At the time of its birth, Internet was limited only to a few universities for their research and to the Department of Defense. IPv4 is 32 bits long and offers around 4,294,967,296 (232) addresses. This address space was considered more than enough that time. Given below are the major points that played a key role in the birth of IPv6:

- Internet has grown exponentially and the address space allowed by IPv4 is saturating. There is a requirement to have a protocol that can satisfy the needs of future Internet addresses that is expected to grow in an unexpected manner.
- IPv4 on its own does not provide any security feature. Data has to be encrypted with some other security application before being sent on the Internet.
- Data prioritization in IPv4 is not up to date. Though IPv4 has a few bits reserved for Type of Service or Quality of Service, but they do not provide much functionality.
- IPv4 enabled clients can be configured manually or they need some address configuration mechanism. It does not have a mechanism to configure a device to have globally unique IP address.

Basic Structure of IPv6

An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbols. For example, given below is a 128 bit IPv6 address represented in binary format and divided into eight 16-bits blocks:

0010000000000001 0000000000000000
0011001000111000 1101111111100001
0000000001100011 0000000000000000
0000000000000000 1111111011111011

Each block is then converted into Hexadecimal and separated by ':' symbol: 2001:0000:3238:DFE1:0063:0000:0000:FEFB. Even after converting into Hexadecimal format, IPv6 address remains long. IPv6 provides some rules to shorten the address. The rules are as follows: Rule.1: Discard leading Zero(es): In Block 5, 0063, the leading two 0s can be omitted, such as (5th block): 2001:0000:3238:DFE1:63:0000:0000:FEFB Rule.2: If two of more blocks contain consecutive zeroes, omit them all and replace with double colon sign ::, such as (6th and 7th block): 2001:0000:3238:DFE1:63::FEFB. Consecutive blocks of zeroes can be replaced only once by :: so if there are still blocks of zeroes in the address, they can be shrunk down to a single zero, such as (2nd block): 2001:0:3238:DFE1:63::FEFB

Migration from IPv4 to IPv6

Listed below are four steps organizations should take when planning an IPv6 migration.

Step 1: IPv6 cost-benefit analysis: The first step in planning an IPv6 migration is to complete a cost-benefit analysis. This is important because at any time during an IPv6 project, this can be required to prevent pushback from the project moving forward. All stakeholders should receive this analysis. It can help with obtaining resources for the project and ensures management at all levels can clearly see the benefits of the project. Many IPv6 projects get put on hold during the implementation when minor issues occur due to management not understanding the benefits of moving forward with it.

Step 2: Readiness assessment: An inventory of the existing infrastructure should be completed. This would include a list of all infrastructure IPv4 addresses in the network, a list of where they are referred to within all applications, and a list of all DNS mappings. This assessment would verify if the current external DNS provider supports IPv6 and if the infrastructure devices supports IPv6.

During this assessment, applications should be evaluated to determine if they will support an IPv6 transition. You should also evaluate the skills of IT employees who will support IPv6. Any training that is required should be documented.

Step 3: Decide what to do with unsupported applications and infrastructure: All applications and infrastructure devices that do not support IPv6 should be documented. The process and cost required to upgrade them to support IPv6 should be documented and presented to management. A decision should be made on whether these devices and applications should be immediately upgraded to support IPv6. This is a critical step to make in defining scope of an IPv6 migration.

Step 4: Plan the details of the migration: Once the initial analysis is complete, organizations must decide whether to move forward with a complete IPv6 cut-over or if a dual-stack implementation makes more sense.

A dual-stack IPv6 migration gives organizations more flexibility because it allows time to gradually convert the network from IPv4 to IPv6. The issues with dual-stack is that it does add a layer of complexity to the network, and you must verify that your network infrastructure equipment supports it.

4.3 Installation of 2008 Enterprise Server

These steps describe the installation of Windows Server 2008 R2 Enterprise (Full Edition).These steps are included to demonstrate ground-up installations of an Infinity application in a two machine and three machine scenario:

1. Insert the installation media for Windows Server 2008 R2. After the installer runs, the Install Windows screen appears.
2. Enter language and other preferences. Click Next.
3. Click Install now. The setup begins. The installer prompts to select an operation system.
4. Select Windows Server 2008 R2 Enterprise (Full Installation) and click Next. The installer prompts to read the license terms.
5. Read the license terms. If you agree to the license terms, select I accept the license terms and click Next.
6. The installer asks you which type of installation. For a new installation, click Custom (advanced).
7. The installer asks for disk location information. Make your selection and click Next.
8. The installation begins.
9. The installer prompts to change the password. Click OK.
10. Enter a new password, re-enter the password to confirm it, and click the right-arrow
11. After you click OK on the confirmation screen, the operating system prepares your desktop.

4.4 Various Edition of Windows 2008 Server

Windows Server 2008 Standard Edition

Windows Server 2008 Standard is one of Microsoft's entry level server offerings (alongside Windows Web Server 2008) and is one of the least expensive of the various editions available. Only a 64-bit versions are available, and in terms of hardware Standard Edition supports up to 32GB of RAM and 4 processors. Windows Server 2008 is primarily targeted and small and mid-sized businesses (SMBs) and is ideal for providing domain, web, DNS, remote access, print, file and application services. Support for clustering, however, is notably absent from this edition. An upgrade path to Windows Server 2008 Standard is available from Windows 2000 Server and Windows Server 2003 Standard Edition.

Windows Server 2008 Enterprise Edition

<google>ADSDAQBOX_FLOW</google> Windows Server 2008 Enterprise Edition provides greater functionality and scalability than the Standard Edition. As with Standard Edition, only a 64-bit version is available. Enhancements include support for as many as 8 processors and up to 2TB of RAM. Additional features of the Enterprise edition include support for clusters of up to 8 nodes and Active Directory

Federated Services (AD FS). Windows Server 2000, Windows 2000 Advanced Server, Windows Server 2003 Standard Edition and Windows Server 2003 Enterprise Edition may all be upgraded to Windows Server 2008 Enterprise Edition.

Windows Server 2008 Datacenter Edition

The Datacenter edition represents the top end of the Windows Server 2008 product range and is targeted at mission critical enterprises requiring stability and high uptime levels. Windows Server 2008 Datacenter edition is tied closely to the underlying hardware through the implementation of custom Hardware Abstraction Layers (HAL). As such, it is currently only possible to obtain Datacenter edition as part of a hardware purchase. As with other versions, the Datacenter edition is available only in a 64-bit version and supports up to 2TB of RAM. In addition, this edition supports a minimum of 8 processors up to a maximum of 64. Upgrade paths to Windows Server 2008 Datacenter Edition are available from the Datacenter editions of Windows 2000 and 2003.

Windows Web Server 2008

Windows Web Server 2008 is essentially a version of Windows Server 2008 designed primarily for the purpose of providing web services. It includes Internet Information Services (IIS) 7.0 along with associated services such as Simple Mail Transfer Protocol (SMTP) and Telnet. It is available in a 64-bit version only and supports up to 4 processors. RAM is limited to 32GB. Windows Web Server 2008 lacks many of the features present in other editions such as clustering, BitLocker drive encryption, multipath I/O, Windows Internet Naming Service (WINS), Removable Storage Management and SAN Management.

4.5 Installation and Configuration of Active Directory

About Active Directory: Active Directory (AD) is a directory service that Microsoft developed for the Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Initially, Active Directory was only in charge of centralized domain management. Starting with Windows Server 2008, however, Active Directory became an umbrella title for a broad range of directory-based identity-related services. A server running Active Directory Domain Services (AD DS) is called a domain controller. It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user. Also, it allows management and storage of information, provides authentication and authorization mechanisms, and establishes a framework to deploy other related services: Certificate Services, Active Directory Federation Services, Lightweight Directory Services and Rights Management Services.

Installation Steps: Now that you have prepared the server, you can install AD DS (DCPROMO). Note: As an alternative to performing steps 1 through 3, you can type dcpromo.exe at the command prompt. Then, skip to step 4.

1. Open the Server Manager window.
2. Select Roles > Active Directory Domain Services.
3. In the Summary section, click Run the Active Directory Domain Services Installation Wizard (dcpromo.exe).
4. On the Welcome page of the Active Directory Domain Services Installation Wizard, ensure that the Use advanced mode installation check box is cleared, and then click Next.
5. On the Operating System Compatibility page, click Next.
6. On the Choose a Deployment Configuration page, select Create a new domain in a new forest and then click Next.

7. On the Name the Forest Root Domain page, enter the domain name that you choose during preparation steps. Then, click Next. The installation program verifies the NetBIOS name.
8. On the Set Forest Functional Level page, select Windows Server 2008 R2 in the Forest function level list. Then, click Next. The installation program examines and verifies your DNS setting.
9. On the Additional Domain Controller Options page, ensure that the DNS server check box is selected, and then click Next.
10. In the message dialog box that appears, click Yes.
11. On the Location for Database, Log Files, and SYSVOL page, accept the default values and then click Next.
12. On the Directory Services Restore Mode Administrator Password page, enter the domain administrator password that you chose during the preparation steps. This is not your admin password that was emailed to you during the creation of your server, although you can use that password if you want to. Then, click Next.
13. On the Summary page, review your selections and then click Next. The installation begins. Note: If you want the server to restart automatically after the installation is completed, select the Reboot on completion check box.
14. If you did not select the Reboot on completion check box, click Finish in the wizard. Then, restart the server.
15. After a few minutes, reconnect to your server in the Console in the Cloud Control Panel or RDP.

Domains: The Active Directory framework that holds the objects can be viewed at a number of levels. The forest, tree, and domain are the logical divisions in an Active Directory network. Within a deployment, objects are grouped into domains. The objects for a single domain are stored in a single database (which can be replicated). Domains are identified by their DNS name structure, the namespace. A domain is defined as a logical group of network objects (computers, users, devices) that share the same Active Directory database.

Trees: A tree is a collection of one or more domains and domain trees in a contiguous namespace, and is linked in a transitive trust hierarchy.

Forests: At the top of the structure is the forest. A forest is a collection of trees that share a common global catalog, directory schema, logical structure, and directory configuration. The forest represents the security boundary within which users, computers, groups, and other objects are accessible.

4.6 Accounts

Users, groups, and computers are the key objects in Active Directory directory service because they allow workers, their managers, system administrators—anyone using a computer on the network—to establish their identity on the network as a security principal. Without this identification, personnel cannot gain access to the computers, applications, and data needed to do their daily work. Although it is true that the minimal identification required is that of a user and computer, management of individual user security principals becomes needlessly complicated unless users are organized into groups. Assigning permissions to hundreds of users individually is not scalable; wise use of groups makes the process of creating and administering permissions much easier.

User: A user's identity is integrated into the Active Directory user object. The user object includes not just the user's name, password, and SID, but also contact information such as telephone numbers and addresses; organizational information including job title, direct reports and manager; group memberships; and configuration such as roaming profile, terminal services, remote access, and remote control settings. This lesson will review and enhance your understanding of user objects in Active Directory.

Group: Groups are objects that can include user, computer, and other group objects as members. When security permissions are set for a group in the access control list (ACL) on a resource, all members of that group receive those permissions. Windows Server 2008 has two group types: security and distribution. Security groups are used to assign permissions for access to network resources. Distribution groups are used to combine users for e-mail distribution lists. Security groups can be used as an email distribution list, but distribution groups cannot be in an ACL. Proper planning of group structure affects maintenance and scalability, especially in an enterprise environment, in which multiple organizational units (OUs), domains, or forests are involved.

Computer: Before you can log on to a computer with your domain user account, that computer must belong to a domain. The two steps necessary to join a computer to a domain are, first, to create an account for the computer and, second, to configure the computer to join the domain using that account. This lesson will focus on the skills related to the creation of computer accounts and joining computers to domains. The next lesson will explore, in more depth, the computer accounts themselves. Just as users do, computers maintain identities, also called "accounts," that include a name, password, and security identifier (SID). Those properties are incorporated into the computer object class within Active Directory. Preparing for a computer to be part of your domain is therefore a process strikingly similar to preparing for a user to be part of your domain: you must create a computer object in Active Directory.

4.7 Policy

Active Directory on Windows Server 2008 supports security policies to strengthen passwords and their use within an enterprise. Of course, you must design a password policy that is sufficiently daunting to attackers while being sufficiently convenient for users, so that they do not forget passwords (resulting in increased calls to the help desk) or, worse, write down their passwords. A system running Windows Server 2008 as a member server maintains a policy related to its local user accounts. The local security policy can be managed using the appropriately named snap-in: Local Security Policy.

Security Policies

Active Directory on Windows Server 2008 supports security policies to strengthen passwords and their use within an enterprise. Of course, you must design a password policy that is sufficiently daunting to attackers while being sufficiently convenient for users, so that they do not forget passwords (resulting in increased calls to the help desk) or, worse, write down their passwords.

- **Password Policy:** The domain password policies enable you to protect your network against password compromise by enforcing best-practice password management techniques.
- **Account Lockout Policy:** Account lockout refers, in its broadest sense, to the concept that after several failed logon attempts by a single user, the system should assume that an attacker is attempting to compromise the account by discovering its password and, in defence, should lock the account so no further logons may be attempted. Domain account lockout policies determine the limitations for invalid logons, expressed in a number of invalid logons in a period of time, and the requirements for an account to become unlocked, whether by simply waiting or by contacting an administrator.

Audit Policies

The following policies are located in the Computer Configuration, Windows Settings, Security Settings, Local Policies, Audit Policy node of Group Policy Object Editor (or the Local Security Policy snap-in). You can configure auditing for successful or failed events.

- **Audit Account Management** Configures auditing of activities, including the creation, deletion, or modification of user, group, or computer accounts. Password resets are also logged when account management auditing is enabled.
- **Audit Account Logon Events** This policy audits each instance of user logon that involves domain controller authentication. For domain controllers, this policy is defined in the Default Domain Controllers GPO. Note, first, that this policy will create a Security log entry on a domain controller each time a user logs on interactively or over the network using a domain account. Second, remember that to evaluate fully the results of the auditing, you must examine the Security logs on all domain controllers because user authentication is distributed among each domain controller in a site or domain.
- **Audit Logon Events** Logon events include logon and logoff, interactively or through network connection. Account logon events are generated on the local computer for local accounts and on the domain controller for network accounts, whereas logon events are generated wherever the logon occurs. If you have enabled Audit Logon Events policy for successes on a domain controller, workstation logons will not generate logon audits. Only interactive and network logons to the domain controller itself generate logon events.

4.8 Logging Event

Windows Server 2008 maintains a variety of logs that contain information about its ongoing processes. To view these logs, you use the Event Viewer Microsoft Management Console (MMC) snap-in. Event Viewer can function as either a stand-alone or an extension snap-in. By configuring the options on each of the logs to meet the requirements of your environment, you can collect data appropriate for troubleshooting hardware, application, system, and resource access. The Windows Server 2003 Event Log service, present and started automatically on all computers running Windows Server 2008, records events in one of three log files:

Application: Contains information about specific programs running on the computer, as determined by the application's developers.

System: Contains information about events generated by Windows Server 2008 components such as services and device drivers. For example, a failure of a service to start or a driver to load during system start-up is recorded in the System log. The types of events recorded in this log are preconfigured by the operating system and cannot be changed. This is the primary Windows Server 2008 log; when you are looking for information about system problems, you should always view this log first.

Security: Can contain information about security-related events such as failed logons, attempts to access protected resources (such as printers, files, and folders), and success or failure of audited events. In its default configuration, Windows Server 2008 does not record information in the Security log. The events recorded in this log are determined by audit policies, which you can enable using either local computer policies or group policies. By default, only members of the Administrators group can view this log.

4.9 MMC (Microsoft Management Console)

The MMC provides a two-paned framework consisting of a console tree pane, also called a scope pane, and a details pane. The MMC menus and a toolbar provide commands for manipulating the parent and child windows, snap-ins, and the console itself. Note that the console has a name and that there is a Console Root. This Console Root will contain any snap-ins that you choose to include. Each console includes a console tree, console menu and toolbars, and the details pane. The contents of these will vary, depending on the design and features of the snap-in you use. Although each snap-in will add its unique menu and toolbar items, there are several key menus and commands that you will use in many situations that are common to most snap-ins. Each MMC contains a collection of one or more tools called snap−ins. A snap-in

extends the MMC by adding specific management capability and functionality. There are two types of snap-ins: stand-alone and extension.

Stand-Alone Snap-Ins: Stand−alone snap−ins are provided by the developer of an application. All administrative tools for Windows Server 2008, for example, are either single snap-in consoles or consoles with a combination of snap-ins useful to a particular task. The File Server Management console (Filesvr.msc), for example, contains snap-ins to facilitate the configuration, monitoring, and optimization of file server storage and shares.

Extension Snap-Ins: Extension snap−ins, or extensions, are designed to work with one or more stand-alone snap-ins. When you add an extension, Windows Server 2008 places the extension into the appropriate location within the stand-alone snap-in. Many snap-ins can act as a stand-alone snap-in or extend the functionality of other snap-ins. For example, the Event Viewer snap-in can operate as a stand-alone snap-in, as in the Event Viewer console, and is an available extension for the Computer Management snap-in.

Unit-5

Basic of Network Security, Internet Connection Sharing

5.1 Fundamental of Network Security

We live in an age of information. Ignoring the fact that you're reading this on a computer screen right now, very little you do doesn't involve computers somehow. Now, with many devices communicating with each other over wired, wireless, or cellular networks, network security is an important concept. In simple terms, network security is securing the network. Easy enough, right? Network security actually includes a few concepts that might surprise you and can be as simple as passwords or as complex as corporate disaster recovery. Studying for the CISSP, a well-known industry certification taken by many who deal in network security also includes elements of law, management of personnel, and even physical security. Security operators might work with locksmiths, construction engineers, lawyers, and other professionals to bring the whole concept together. At its core, network security refers to three core elements, known as the **CIA Model**:

Confidentiality: Only those who are supposed to access the data can access it. We use the term 'access' because we're not just talking about reading it, but any form of interaction with the data should be by those who have proper authority.

Integrity: The data that's there is only changed when it's supposed to be. A good example is a scene you might have seen in a movie in which a student sneaks into school and changes his grades. In this case, the file with his grades has reduced integrity since it can't be trusted to be accurate.

Availability: The data is there when it is needed. This may seem strange in the view of security, but remember that data in network security is the same as money in a bank vault. Is your vault secure if someone can walk in and take money out without authority?

Now, all of that is about access, or any sort of usage of data or the devices containing that data. That's why understanding the elements of access is so important. Guess what, there is a list for that.

Authentication: You are who you say you are. While there can be various forms of identification used, authentication is usually through a PIN like your debit card uses or the login on your email account.

Authorization: You are where you're supposed to be. Try walking into a secured area without a good reason and permission, and see how that works out for you. Probably not well.

Accounting: Professionals sometimes call this logging. This means that everything you do is properly noted, and any changes to data can be tied to a user account. To go back to the debit card example, this would be your bank statement.

5.2 Security Methods

Encryption/Cryptography: In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating ciphertext that can be read only if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

Authentication: Authentication is the act of confirming the truth of an attribute of a single piece of data claimed true by an entity. In contrast with identification, which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of

actually confirming that identity. It might involve confirming the identity of a person by validating their identity documents, verifying the authenticity of a website with a digital certificate, determining the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labeling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification.

5.4 Internet Technology

Dialup

Dialup network use modem to connect one computer with the other. A modem (portmanteau of modulator-demodulator) is a hardware device that converts data between transmission media so that it can be transmitted from computer to computer (historically over telephone wires). The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used with any means of transmitting analog signals from light-emitting diodes to radio. A common type of modem is one that turns the digital data of a computer into modulated electrical signal for transmission over telephone lines and demodulated by another modem at the receiver side to recover the digital data.

ISDN

Integrated Services Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. It was first defined in 1988 in the CCITT red book. Prior to ISDN, the telephone system was viewed as a way to transport voice, with some special services available for data. The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system. The ISDN standards define several kinds of access interfaces, such as Basic Rate Interface (BRI), Primary Rate Interface (PRI), Narrowband ISDN (N-ISDN), and Broadband ISDN (B-ISDN).

ISDN is a circuit-switched telephone network system, which also provides access to packet switched networks, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in potentially better voice quality than an analog phone can provide. It offers circuit-switched connections (for either voice or data), and packet-switched connections (for data), in increments of 64 kilobit/s. In some countries, ISDN found major market application for Internet access, in which ISDN typically provides a maximum of 128 kbit/s bandwidth in both upstream and downstream directions. Channel bonding can achieve a greater data rate; typically the ISDN B-channels of three or four BRIs (six to eight 64 kbit/s channels) are bonded. ISDN is employed as the network, data-link and physical layers in the context of the OSI model. In common use, ISDN is often limited to usage to Q.931 and related protocols, which are a set of signaling protocols establishing and breaking circuit-switched connections, and for advanced calling features for the user. They were introduced in 1986.

Leas line

A leased line is a private bidirectional or symmetric telecommunications circuit between two or more locations provided in exchange for a monthly rent. Sometimes known as a private circuit or data line in the UK. Unlike traditional PSTN lines they do not have telephone numbers, each side of the line being permanently connected and dedicated to the other. Leased lines can be used for telephone, Internet, or other data services. Some are ringdown services, and some connect to a private branch exchange or router.

Typically, leased lines are used by businesses to connect geographically distant offices. Unlike dial-up connections, a leased line is always active. The fee for the connection is a fixed monthly rate. The primary factors affecting the monthly fee are distance between end points and the speed of the circuit. Because the connection does not carry anybody else's communications, the carrier can assure a given level of

quality. An Internet leased line is a premium Internet connectivity product, normally delivered over fiber, which provides uncontended, symmetrical speeds with full duplex. It is also known as an ethernet leased line, dedicated line, data circuit or private line.

5.5 VPN

A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network. VPN technology was developed to allow remote users and branch offices to access corporate applications and resources. To ensure security, the private network connection is established using an encrypted layered tunneling protocol and VPN users use authentication methods, including passwords or certificates, to gain access to the VPN. In other applications, Internet users may secure their transactions with a VPN, to circumvent geo-restrictions and censorship, or to connect to proxy servers to protect personal identity and location to stay anonymous on the Internet. However, some websites block access to known VPN technology to prevent the circumvention of their geo-restrictions, and many VPN providers have been developing strategies to get around these roadblocks.

A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunneling protocols over existing networks. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.

5.5.1 Types of VPN

VPN is a Virtual Private Network that allows a user to connect to a private network over the Internet securely and privately. VPN creates an encrypted connection, known as VPN tunnel, and all Internet traffic and communication is passed through this secure tunnel. Thus, keeping the user data secure and private. There are two basic VPN types which are explained below.

- **Remote Access VPN:** Remote access VPN allows a user to connect to a private network and access its services and resources remotely. The connection between the user and the private network happens through the Internet and the connection is secure and private. Remote Access VPN is useful for business users as well as home users. A corporate employee, while traveling, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network. Home users, or private users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users conscious of Internet security also use VPN services to enhance their Internet security and privacy.
- **Site – to – Site VPN:** A Site-to-Site VPN is also called as Router-to-Router VPN and is mostly used in the corporates. Companies, with offices in different geographical locations, use Site-to-site VPN to connect the network of one office location to the network at another office location. When multiple offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN. When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN. Basically, Site-to-site VPN create a virtual bridge between the networks at geographically distant offices and connect them through the Internet and maintain a secure and private communication between the networks. Since Site-to-site VPN is based on Router-to-Router communication, in this VPN type one router acts as a VPN Client and another router as a VPN Server. The communication between the two routers starts only after an authentication is validated between the two.

5.5.2 Use of VPN

5.5.3 VPN Protocol

The above two VPN types are based on different VPN security protocols. Each of these VPN protocols offer different features and levels of security, and are explained below:

Internet Protocol Security or IPSec: Internet Protocol Security or IPSec is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by authenticating the session and encrypts each data packet during the connection. IPSec operates in two modes, Transport mode and Tunneling mode, to protect data transfer between two different networks. The transport mode encrypts the message in the data packet and the tunneling mode encrypts the entire data packet. IPSec can also be used with other security protocols to enhance the security system.

Layer 2 Tunneling Protocol (L2TP): L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is usually combined with another VPN security protocol like IPSec to create a highly secure VPN connection. L2TP creates a tunnel between two L2TP connection points and IPSec protocol encrypts the data and handles secure communication between the tunnel.

Point – to – Point Tunneling Protocol (PPTP): PPTP or Point-to-Point Tunneling Protocol creates a tunnel and encapsulates the data packet. It uses a Point-to-Point Protocol (PPP) to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the time of Windows 95. Apart from Windows, PPTP is also supported on Mac and Linux.

5.6 Proxy Server

In computer networks, a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems. A proxy server may reside on the user's local computer, or at any point between the user's computer and destination servers on the Internet. A proxy server that passes unmodified requests and responses is usually called a gateway or sometimes a tunneling proxy. A forward proxy is an Internet-facing proxy used to retrieve data from a wide range of sources (in most cases anywhere on the Internet). A reverse proxy is usually an internal-facing proxy used as a front-end to control and protect access to a server on a private network. A reverse proxy commonly also performs tasks such as load-balancing, authentication, decryption or caching.

5.7 Firewall

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet. Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines.

Types of Firewall

Firewalls are generally categorized as network-based or host-based. Network-based firewalls are positioned on the gateway computers of LANs, WANs and intranets. They are either software appliances running on general-purpose hardware, or hardware-based firewall computer appliances. Firewall appliances may also offer other functionality to the internal network they protect, such as acting as a DHCP or VPN server for that network. Host-based firewalls are positioned on the network node itself and control network traffic in and out of those machines. The host-based firewall may be a daemon or service as a part

of the operating system or an agent application such as endpoint security or protection. Each has advantages and disadvantages. However, each has a role in layered security.

- **Network layer or packet filters:** Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply. The term "packet filter" originated in the context of BSD operating systems. Network layer firewalls generally fall into two sub-categories, stateful and stateless.
- **Application-layer:** Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or FTP traffic), and may intercept all packets traveling to or from an application. Application firewalls function by determining whether a process should accept any given connection. Application firewalls accomplish their function by hooking into socket calls to filter the connections between the application layer and the lower layers of the OSI model. Application firewalls that hook into socket calls are also referred to as socket filters. Application firewalls work much like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a per port basis. Generally, prompts are used to define rules for processes that have not yet received a connection. It is rare to find application firewalls not combined or used in conjunction with a packet filter.
- **Network address translation:** Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range", as defined in RFC 1918. Firewalls often have such functionality to hide the true address of computer which is connected to the network. Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization. Although NAT on its own is not considered a security feature, hiding the addresses of protected devices has become an often used defense against network reconnaissance.

5.8 GPS

The Global Positioning System (GPS), originally Navstar GPS, is a satellite-based radionavigation system owned by the United States government and operated by the United States Air Force. It is a global navigation satellite system that provides geolocation and time information to a GPS receiver anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites. Obstacles such as mountains and buildings block the relatively weak GPS signals.

The GPS does not require the user to transmit any data, and it operates independently of any telephonic or internet reception, though these technologies can enhance the usefulness of the GPS positioning information. The GPS provides critical positioning capabilities to military, civil, and commercial users around the world. The United States government created the system, maintains it, and makes it freely accessible to anyone with a GPS receiver.

The GPS project was launched in the United States in 1973 to overcome the limitations of previous navigation systems, integrating ideas from several predecessors, including classified engineering design studies from the 1960s. The U.S. Department of Defense developed the system, which originally used 24 satellites. It was initially developed for use by the United States military and became fully operational in 1995. Civilian use was allowed from the 1980s. Roger L. Easton of the Naval Research Laboratory, Ivan A. Getting of The Aerospace Corporation, and Bradford Parkinson of the Applied Physics Laboratory are credited with inventing it. The work of Gladys West is credited as instrumental in the development of computational techniques for detecting satellite positions with the precision needed for GPS. The design of

GPS is based partly on similar ground-based radio-navigation systems, such as LORAN and the Decca Navigator, developed in the early 1940s.

5.9 GPRS

General Packet Radio Service (GPRS) is a packet oriented mobile data standard on the 2G and 3G cellular communication network's global system for mobile communications (GSM). GPRS was established by European Telecommunications Standards Institute (ETSI) in response to the earlier CDPD and i-mode packet-switched cellular technologies. It is now maintained by the 3rd Generation Partnership Project (3GPP). GPRS is typically sold according to the total volume of data transferred during the billing cycle, in contrast with circuit switched data, which is usually billed per minute of connection time, or sometimes by one-third minute increments. Usage above the GPRS bundled data cap may be charged per MB of data, speed limited, or disallowed.

GPRS is a best-effort service, implying variable throughput and latency that depend on the number of other users sharing the service concurrently, as opposed to circuit switching, where a certain quality of service (QoS) is guaranteed during the connection. In 2G systems, GPRS provides data rates of 56–114 kbit/sec. 2G cellular technology combined with GPRS is sometimes described as 2.5G, that is, a technology between the second (2G) and third (3G) generations of mobile telephony. It provides moderate-speed data transfer, by using unused time division multiple access (TDMA) channels in, for example, the GSM system. GPRS is integrated into GSM Release 97 and newer releases. The GPRS core network allows 2G, 3G and WCDMA mobile networks to transmit IP packets to external networks such as the Internet. The GPRS system is an integrated part of the GSM network switching subsystem.

5.10 CCTV

Closed-circuit television (CCTV), also known as video surveillance, is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. It differs from broadcast television in that the signal is not openly transmitted, though it may employ point to point (P2P), point to multipoint (P2MP), or mesh wired or wireless links. Though almost all video cameras fit this definition, the term is most often applied to those used for surveillance in areas that may need monitoring such as banks, stores, and other areas where security is needed. Though Videotelephony is seldom called 'CCTV' one exception is the use of video in distance education, where it is an important tool.

The term DVR implies Digital Video Recorder. It is an innovative gadget that transforms the analog signals from a CCTV or Closed Circuit Camera into digital format, keeps or maintains the information in a hard drive and transmits live video stream to other devices or gadgets on the same network. A Closed Circuit Camera, which has a DVR is not completely analog. The CCTV transmits the video signal in an analog format and the connected DVR transmits the received signals to the digital format prior to recording and sending over the respective network. Therefore, while you are using a CCTV project, which has minimum one DVR, your CCTV is not essentially analog. It is in reality a hybrid CCTV project.

Uses:

- Crime prevention
- Industrial processes
- Traffic monitoring
- Transport safety
- Monitor employees
- Use in schools