UNIT 1

Chapter 1: Introduction

❖ What is Network? :

A network is the most cost-effective way to share a collection of communication equipment such as PC's, servers, printers, and modems that has been connected together by cables. A network helps people work collectively, not just individually.

❖ Network Concept :

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

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)

Having a transmission pathway does not always guarantee communication. When two entities communicate, they do not merely exchange information; rather, they must understand the information they receive from each other. The goal of computer networking, therefore, is not simply to exchange data but to understand and use data received from other entities on the network.

The two main reasons for using computer networking are to provide services and to reduce equipment costs. Networks enable computers to share their resources by offering services to other computers and users on a network.

The following are specific reasons for networking PCs:

- Sharing files
- Sharing printers and other devices
- Enabling centralized administration and security of the resources within the system
- Supporting network applications such as electronic mail and database services

❖ Types of Networks :

- LAN – Local Area Network
- MAN – Metropolitan Area Network
- WAN – Wide Area Network

❖ LAN (Local Area Network)

- A local area network may serve as few as two or three users (for example, in a home network) or many as thousands of users.
- Local-area networks (LANs) evolved around the PC revolution. LANs enabled multiple users in a relatively small geographical area to exchange files and messages, as well as to access shared resources such as file servers and printers.

- Is a group of computers and associated device that share a common communications line or wireless link and typically share the resources of a single processor or server within a small geographic area (for example, within an College Building).

LANs are characterized by the following:

- They transfer data at high speeds (higher bandwidth).
- They exist in a limited geographical area.
- Connectivity and resources, especially the transmission media, usually are managed by the company running the LAN.

❖ MAN - (Metropolitan-area networks)

- A MAN usually consists of two or more LANs in a common geographic area. Typically, a service provider is used to connect two or more LAN sites using private communication lines or optical services. A MAN can also be created using wireless bridge technology by beaming signals across public areas.

❖ WAN – (Wide Area Network)

- WANs interconnect LANs, which then provide access to computers or file servers in other locations. Because WANs connect user networks over a large geographical area, they make it possible for businesses to communicate across great distances. WANs allow computers, printers, and other devices on a LAN to be shared with distant locations.

WANs are characterized by the following:

- They exist in an unlimited geographical area.
- They usually interconnect multiple LANs.
- They often transfer data at lower speeds (lower bandwidth).
- Connectivity and resources, especially the transmission media, usually are managed by a third-party carrier such as a telephone or cable company.

❖ Network Model :

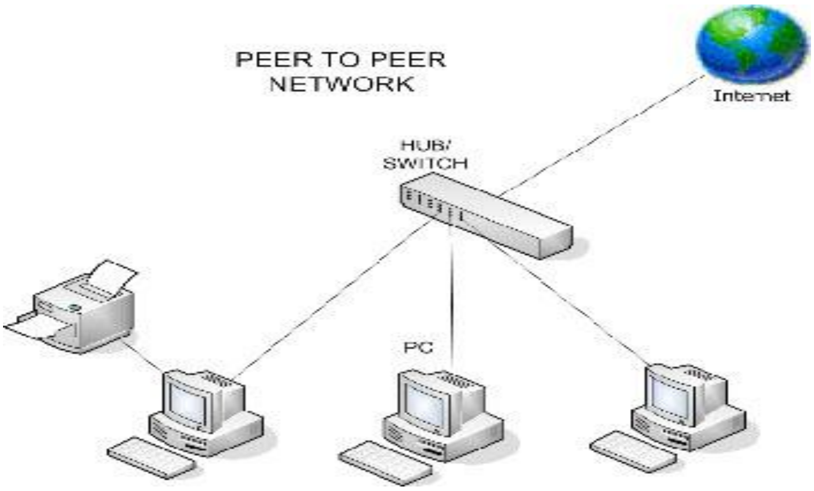
- Networks are all about sharing resources of computers, servers, printers, scanners etc to each other. There are two different types with which network between computers can be formed. Networking formation completely depends on the requirement of the organization scale and usability. We should always study requirements and needs before we decide to choose any type of network. Picking wrong set of options can cost you waste of money, time and resources.
- Two types of networks are Peer to Peer networking also known to be p2p, the other one is Client and Server networks.
- (1) Peer to Peer (2) Client Server

(1) Peer to Peer (p2p) Model:

- P2p networking type is most commonly used computer networks. This type of network is very cost effective but supports lesser number of computers in network. Ten to fifteen computers can be connected to each other using p2p networking model without problem, more number of computers often create problems.
- All computers possesses same status within the network and no computer control any other computer but it self, this network does not have server to control and monitor.
- Security level is not towards higher side and each work station it self is responsible for security. Using p2p models files can be shared

among computers. Files like, videos, audios, pictures, spreadsheets and all digital media can be sent or received with in the network.

- Printers, scanners and internet can be shared with in all computers.
- Below is the picture showing three computers connected to each other with hub and switch. All computers are connected to hub through Network adaptor card using Cable and hub or switch is connected to internet to pass it on to connected computers.. You can see there is no server involved in this diagram but all individual computers are connecting to hub forming P2P network.



Limitation of P2P networking model:

Before deciding to implement P2P model one must know the limitations of this type. Getting to know later can be frustrating big time. It would highly be recommended to get your organizational people site together and discuss the needs. Peer to Peer looks very simple, quite cost effective and attractive, yet it can keep progress very limited.

- Peer-To-Peer networks are designed for limited number computers, it will start creating issues when exceed 15 number of computers
- High security levels can not be achieved using p2p networks, so if organization have concerns with security p2p will not be that great.
- Organizational growth will outgrow p2p networks; it will not support growing number of computers when increased above fifteen.
- Regular training is required for computer users of p2p network. p2p network is control by computers and computers are controlled by human, small mistake by one of the user can hold the work for other users on same p2p network.

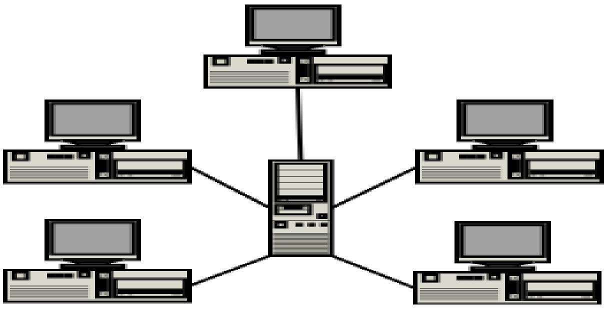
(2) Client Server Model:

- Choosing right kind of networking model is very important for organization. If you are using lesser number of computer and do not see any need to increase the numbers of computers to more than 15 then you are fine with peer to peer networking model, but if you are bigger organization or seeing growth in network, client and server model is designed for it.
- The difference in p2p and client server model is that p2p does not have any device or computer that controls computers on network whereas; client / server model has one dedicated computer which is called

server. It is called dedicated server. All computers are connected to hub and hub is connected to dedicated server.

- Server is responsible to perform according to the request sent to it by clients. For example server can act as print server, if client request a print of document server will send print command to printer and it will be printed.
- Same way all the files are stored on the server and not on client computer, same client can retrieve data by using any other computer on the same network. This concept is known as centralization, this enables server to keep profile of users, data, and software etc completely in tacked and organized.
- Normal computer can also be configured as server and it should be alright and perform server tasks efficiently, but if network growth is on seen and many computers are required to attach to network that's where we might need proper server to take over the network.
- You can see in diagram below. All the workstations (Clients) are attached on server, some times there is hub involved but in this case it is just clients and server.

Client Server model



❖ Peer-to-Peer versus Client/ Server Networks :

Advantages

Peer-to-Peer Networks

- No dedicated server.
- Less expensive.
- Easy to install and maintain.
- Good file, printer, and CD-ROM sharing.

Client/Server Networks

- Fast.
- Expandable.
- Will work with any application.
- Handles shared database applications.
- More reliable (dedicated server).
- Highest level of security.

Disadvantages

Peer-to-Peer Networks

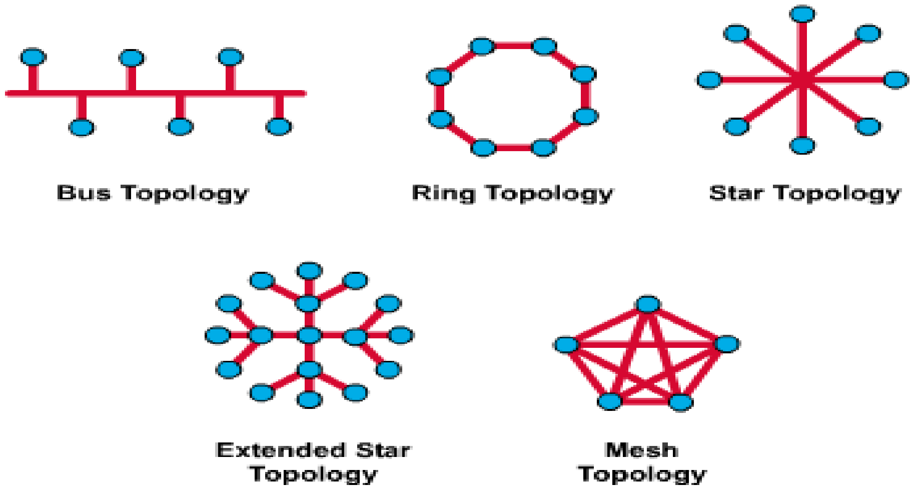
- Slow.
- No good for database applications.
- Less reliable (server is workstation).
- Limited expandability.

Client/Server

- Needs dedicated server.
- More expensive to buy.
- More expensive to maintain.

Network Topology:

- The network topology defines the way in which computers, printers, and other devices are connected. A network topology describes the layout of the wire and devices as well as the paths used by data transmissions.



Bus Topology:

- All devices are connected to a central cable, called the bus or backbone.
- Bus networks are relatively inexpensive and easy to install for small networks.
- Ethernet systems use a bus topology. In Simple way we can say us (All devices share a common wire to transmit and receive data through using an arbitration method.)
- Commonly referred to as a linear bus, all the devices on a bus topology are connected by one single cable.

Advantages:

- It is easy to handle and implement.
- It is best suited for small networks

Disadvantages:

- The cable length is limited. This limits the number of stations that can be connected.
- This network topology can perform well only for a limited number of nodes.

Star & Tree Topology :

- All devices are connected to a central hub.
- Star networks are relatively easy to install and manage, but bottlenecks can occur because all data must pass through the hub.
- This is not much of a problem anymore with the widespread deployment of switches.
- At the central point we usually see a device generically called a hub or switch.
- The star topology is the most commonly used architecture in Ethernet LANs.
- When installed, the star topology resembles spokes in a bicycle wheel.
- Larger networks use the extended star topology also called tree topology.
- This topology significantly reduces the traffic on the wires by sending packets only to the wires of the destination host.

Advantages:

- Due to its centralized nature, the topology offers simplicity of operation.
- It also achieves an isolation of each device in the network.

Disadvantages:

- The network operation depends on the functioning of the central hub. Hence, the failure of the central hub leads to the failure of the entire network.

➢ **Ring topology:**

- All devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it.
- Ring topologies are relatively expensive and difficult to install, but they offer high bandwidth and can span large distances.
- A ring is created to which each device attaches. A special signal, called a token travels around the ring letting it know that it is that device's turn to transmit.

Advantages:

- The data being transmitted between two nodes passes through all the intermediate nodes. A central server is not required for the management of this topology.

Disadvantages:

- The failure of a single node of the network can cause the entire network to fail.
- The movement or changes made to network nodes affects the performance of the entire network.

➢ **Mesh Topology :**

- The mesh topology connects all devices (nodes) to each other for redundancy and fault tolerance.
- It is used in WANs to interconnect LANs and for mission critical networks like those used by banks and financial institutions.
- Implementing the mesh topology is expensive and difficult.

Advantage:

The arrangement of the network nodes is such that it is possible to transmit data from one node to many other nodes at the same time.

Disadvantage:

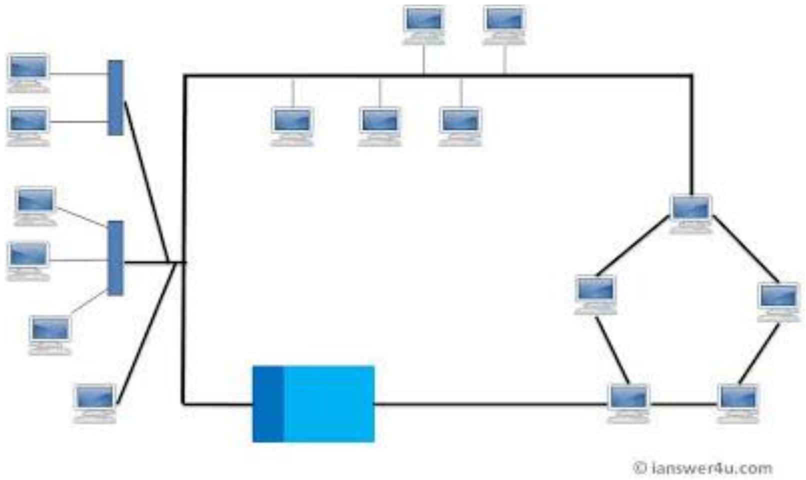
- The arrangement wherein every network node is connected to every other node of the network, many of the connections serve no major purpose. This leads to the redundancy of many of the network connections.

❖ **What is Hybrid Topology?**

Before starting about Hybrid topology, we saw that a network topology is a connection of various links and nodes, communicating with each other for transfer of data. We also saw various advantages and disadvantages of Star, Bus, Ring, Mesh and Tree topologies.

Now lets discuss what Hybrid Network topology is and why it finds its application in Wide Area Networks. Hybrid, as the name suggests, is mixture of two different things. Similarly in this type of topology we integrate two or more different topologies to form a resultant topology which has good points(as well as weaknesses) of all the constituent basic topologies rather than having characteristics of one specific

topology. This combination of topologies is done according to the requirements of the organization.
For example, if there exists a ring topology in one office department while a bus topology in another department, connecting these two will result in Hybrid topology. Remember connecting two similar topologies cannot be termed as Hybrid topology. Star-Ring and Star-Bus networks are most common examples of hybrid network.



Hybrid Network Topology Image

Advantages of Hybrid Network Topology

1) **Reliable:** Unlike other networks, fault detection and troubleshooting is easy in this type of topology. The part in which fault is detected can be isolated from the rest of network and required corrective measures can be taken, WITHOUT affecting the functioning of rest of the network.
2) **Scalable:** Its easy to increase the size of network by adding new components, without disturbing existing architecture.
3) **Flexible:** Hybrid Network can be designed according to the requirements of the organization and by optimizing the available resources. Special care can be given to nodes where traffic is high as well as where chances of fault are high.
4) **Effective:** Hybrid topology is the combination of two or more topologies, so we can design it in such a way that strengths of constituent topologies are maximized while there weaknesses are neutralized. For example we saw Ring Topology has good data reliability (achieved by use of tokens) and Star topology has high tolerance capability (as each node is not directly connected to other but through central device), so these two can be used effectively in hybrid star-ring topology.

- **Disadvantages of Hybrid Topology**

1) **Complexity of Design:** One of the biggest drawback of hybrid topology is its design. Its not easy to design this type of architecture and its a tough job for designers. Configuration and installation process needs to be very efficient.
2) **Costly Hub:** The hubs used to connect two distinct networks, are very expensive. These hubs are different from usual hubs as they need to be intelligent enough to work with different architectures and should be function even if a part of network is down.
3) **Costly Infrastructure:** As hybrid architectures are usually larger

in scale, they require a lot of cables, cooling systems, sophisticate network devices, etc.

ADDITIONAL TOPOLOGIES:-

1- ETHERNET TOPOLOGIES
2- CDDI
3- FDDI

❖ Ethernet TOPOLOGY:-

→ Key features of Ethernet topologies:

- Fast, reliable throughput speed-10 Mbps.
- Accurate transmission-CSMA/CD access method.
- Easy compatibility-more LAN components match Ethernet standards than any other.
- Maximum flexibility-two topologies (bus or star) and five kinds of cable (standard or Thin coax; unshielded twisted pair; FOIRL or 10BASE-FL fibre optic).

❖ Overview:

Ethernet is the most widely used network topology. You can choose between bus and star topologies, as well as coax, twisted-pair, or fibre optic cabling. And with the right connective equipment, multiple Ethernet-based LANs can be linked together. In fact, with the right equipment and software, even Token Ring, AppleTalk®, and wireless LANs can be connected to Ethernet. Ethernet uses CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

In this method, multiple workstations access a transmission medium (multiple access) by listening until no signals are detected (carrier sense). Then they transmit and check to see if more than one signal is present (collision detection). Each station attempts to transmit when it "believes" the network is free. If there is a collision, each station attempts to retransmit after a preset delay, which is different for each workstation. When a collision is detected, a "jam" signal is propagated to all nodes. Each station that detects the collision will wait some period of time and then try again.

→ The two possible topologies for Ethernet are bus and star.

The bus is the simplest (and the traditional) topology. Standard Ethernet (10BASE5) and Thin Ethernet (10BASE2), both based on coax cable systems, use the bus. In this one-cable LAN, all workstations are connected in succession (a "bus" arrangement) on a single cable. All transmissions go to all the connected workstations.

Each workstation then selects the transmissions it should receive based on the address information contained in the transmission.

→ In a star topology, all attached workstations are wired directly to a central hub that establishes, maintains, and breaks connections between them (in the event of an error). The advantage of a star topology is that it's easy to isolate a problem node. The disadvantage is that if the hub fails, the entire system is compromised. Twisted-Pair Ethernet (10BASE-T), based on unshielded twisted pair, and Fibre Optic Ethernet (FOIRL and 10BASE-FL), based on fibre optic cable, use the star.

→ Typical applications.

Use a bus topology for a large network with many users and longer segments. With repeaters or media converters, you can easily interconnect to other networks with different topologies.

→ Use a star topology when you want to use twisted-pair cabling (10BASE-T Ethernet) for a multiple-building campus setup (you might already have twisted pair-telephone wire-installed on your premises). Use a star topology for your fiber optic links.

❖ **CDDI** :-

→ Copper Distributed Data Interface (CDDI) is a standard for data transmission in a local area network. It uses optical fiber as its standard underlying physical medium, although it was also later specified to use copper cable, in which case it may be called FDDI.

→ Description

→ CDDI provides a 100 Mbit/s twisted pair standard for data transmission in local area network that can extend in range up to 200 kilometers (120 mi). Although CDDI logical topology is a ring-based token network, it did not use the IEEE 802.5 token ring protocol as its basis; instead, its protocol was derived from the IEEE 802.4 token bus timed token protocol. In addition to covering large geographical areas, CDDI local area networks can support thousands of users. CDDI offers both a Dual-Attached Station (DAS), counter-rotating token ring topology and a Single-Attached Station (SAS), token bus passing ring topology.

→ A FDDI network contains two rings, one as a secondary backup in case the primary ring fails. The primary ring offers up to 100 Mbit/s capacity. When a network has no requirement for the secondary ring to do backup, it can also carry data, extending capacity to 200 Mbit/s. The single ring can extend the maximum distance; a dual ring can extend 100 km (62 mi). CDDI had a small frame size than the standard Ethernet family, which only supports a maximum-frame size of 1,500 bytes, allowing better effective data rates in some cases.

❖ **FDDI :-**

→ **Fiber Distributed Data Interface** (**FDDI**) is a standard for data transmission in a local area network. It uses optical fiber as its standard underlying physical medium, although it was also later specified to use copper cable, in which case it may be called **CDDI** (Copper Distributed Data Interface), standardized as **TP-PMD** (Twisted-Pair Physical Medium-Dependent), also referred to as TP-DDI (Twisted-Pair Distributed Data Interface).

→ **Description**

→ FDDI provides a 100 Mbit/s optical standard for data transmission in local area network that can extend in range up to 200 kilometers (120 mi). Although FDDI logical topology is a ring-based token network, it did not use the IEEE 802.5 token ring protocol as its basis; instead, its protocol was derived from the IEEE 802.4 token bus timed token protocol. In addition to covering large geographical areas, FDDI local area networks can support thousands of users. FDDI offers both a Dual-Attached Station (DAS), counter-rotating token ring topology and a Single-Attached Station (SAS), token bus passing ring topology.

→ FDDI, as a product of American National Standards Institute X3T9.5 (now X3T12), conforms to the Open Systems Interconnection (OSI) model of functional layering using other protocols. The standards process started in the mid 1980s.

→ DDI-II, a version of FDDI described in 1989, added circuit-switched service capability to the network so that it could also handle voice and video signals. Work started to connect FDDI networks to synchronous optical networking (SONET) technology.

→ A FDDI network contains two rings, one as a secondary backup in case the primary ring fails. The primary ring offers up to 100 Mbit/s capacity. When a network has no requirement for the secondary ring to do backup, it can also carry data, extending capacity to 200 Mbit/s. The single ring can extend the maximum distance; a dual ring can extend 100 km (62 mi). FDDI had a larger maximum-frame size (4,352 bytes) than the standard Ethernet family, which only supports a maximum-frame size of 1,500 bytes, allowing better effective data rates in some cases.

❖ Network Services:

● File services :

File services enable networked computers to share files with each other. This capability was one of the primary reasons networking of personal computers initially came about. File services include all network functions dealing with the storage, retrieval, or movement of data files. File services enable users to read, write, and manage files and data. This includes moving files between computers and archiving files and data.

File services are an important part of client/server and peer-to-peer networks. Computers providing files services are referred to as file servers.

Two types of servers exist:

Dedicated and non-dedicated. Dedicated servers do nothing but fulfill requests to network clients. These servers commonly are found in client/server environments. Non-dedicated servers do double duty. They enable a user to go onto the machine acting as a file server and request the use of files from other machines; at the same time, they give files to users who request them from other computers on the network.

● Printing Services :

After file services, printing is probably the second biggest incentive for installing a LAN.

The following are some of the many advantages of network print services:

- Many users can share the same printers. This capability is especially useful with expensive devices such as color printers and plotters.
- Printers can be located anywhere, not just next to a user's PC.
- Queue-based network printing is more efficient than direct printing because the workstation can begin to work again as soon 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.

● Application Services :

- Application services enable organizations to install servers that are specialized for specific functions
- Some of the more common application servers are database servers, messaging/communication servers, groupware servers, and directory servers. Application servers are an effective strategy for making a network more scalable.
- Additional application servers can be added as new application needs emerge.
- If more power is necessary for an application, only the application server needs to be upgraded.

- Application services enable applications to leverage the computing power and specialized capabilities of other computers on a network.

- **Database Services :**
  - 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 are called client/server databases.
  - With a client/server database, the client and server applications are designed to take advantage of the specialized capabilities of client and database systems,
  - 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 and generates the results required by the client; and transmits results back to the client.
  - The database server can service requests for multiple clients at the same time.

A modern database server is a sophisticated piece of software that can perform the following functions:

- Provide database security.
- Optimize the performance of database operations.
- Determine optimum locations for storing data without requiring clients to know where the data is located.
- Service large numbers of clients by reducing the amount of time any one client spends accessing the database.
- Distribute data across multiple database servers.

- **Messaging/Communication Services :**

Messaging/communication services generally transfer information from one place to another.

This communication of information can be broken down into three subareas:

- Email
- Voice mail
- Fax services

Email:

Email systems can service any size group from a local workgroup to 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. This enables users in dozens of countries throughout the world to exchange electronic messages.

Early text-based email has given way to elaborate systems that support embedded sound, graphics, and even video data.

Some of the major email packages include Microsoft's Exchange Server, Novell's GroupWise, and Lotus Notes.

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 moving

Your voicemail messages from the phone system to the LAN and enabling 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 your can “print” the document to a fax device. Fax services, however, can take on more complicated
Features including the capability to send faxes to a central fax server and to receive faxes from the phone system to a central fax device. That device then delivers the fax message to your PC. This all occurs
Automatically.

- **Security Services :**

- Another service provided by networks is security. Security is one of the most important elements involved
  In a network.
- When users share resources and data on a network, they should be able to control who can access the
  Data or resource and what the user can do with it. An example of this is a file showing the financial records of a company. If this file is on a file server, it is important to be able to control who has access to the file.
- Security services often deal with a user account database or something like the aforementioned directory services. This database of users often contains a list of names and passwords.
  When a person wants to access the network, he must log on to the network. Logging on is similar to trying to enter an office building with a security guard at the front door. Before you can enter the building, you must verify who you are against a list of people who are allowed access.
  Security services often are intermingled with other services. Some services added to a network can utilize the security services of the system onto which they have been installed. An example of this is Microsoft Exchange Server. This messaging product can utilize the security services of an existing Windows NT Server.

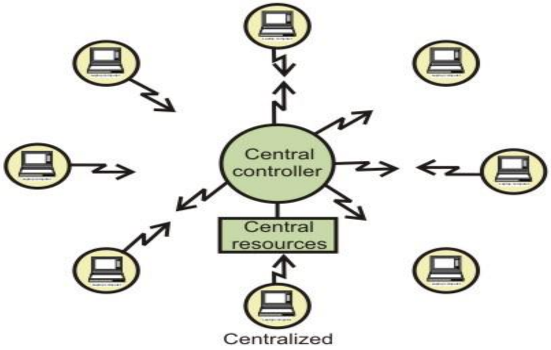
❖ **Network Access Method :**

- A network of computers based on multi-access medium requires a protocol for effective sharing of the media. As only one node can send or transmit signal at a time using the broadcast mode, the main problem here is how different nodes get control of the medium to send data, that is “who goes next?”. The protocols used for this purpose are known as Medium Access Control (MAC) techniques

(1) Polling :

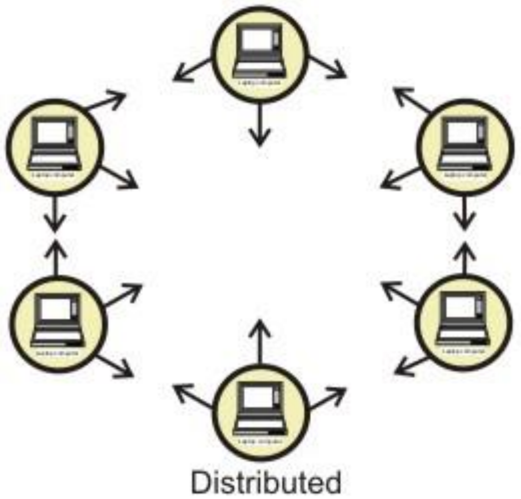
- The mechanism of polling is similar to the roll-call performed in a classroom. Just like the teacher, a controller sends a message to each node in turn.
- The message contains the address of the node being selected for granting access.
- Although all nodes receive the message, only the addressed node responds and then it sends data, if any. If there is no data, usually a “poll reject” message is sent back. In this way, each node is interrogated in a round-robin fashion, one after the other, for granting access to the medium.

- The first node is again polled when the controller finishes with the remaining codes.
- The polling scheme has the flexibility of either giving equal access to all the nodes, or some nodes may be given higher priority than others. In other words, priority of access can be easily implemented.



Polling using a central controller

- Polling can also be accomplished without a central controller. Here, all stations receive signals from other stations as shown in Fig. Below. Stations develop a polling order list, using some protocol.



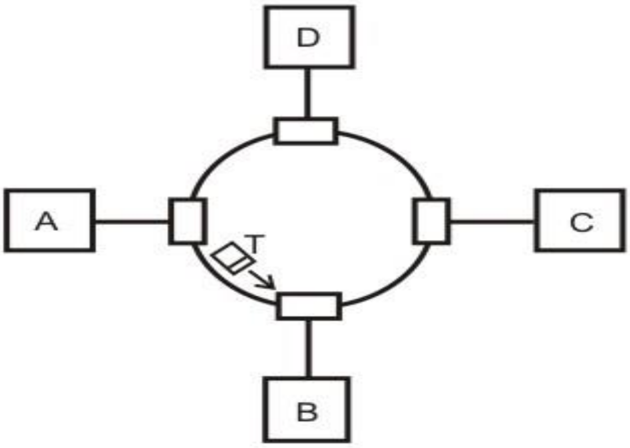
Polling in a distributed manner

(2)**Token Passing**:

- In token passing scheme, all stations are logically connected in the form of a ring and control of the access to the medium is performed using a token. A token is a special bit pattern or a small packet, usually several bits in length, which circulate from node to node. Token passing can be used with both broadcast (token bus) and sequentially connected (token ring) type of networks.
- In case of token ring, token is passed from a node to the physically adjacent node. On the other hand, in the token bus, token is passed with the help of the address of the nodes, which form a logical ring. In either case a node currently holding the token has the 'right to transmit'. When it has got data to send, it removes the token and transmits the data and then forwards the token to the next logical or physical node in the ring. If a node currently holding the token has no data to send, it simply forwards the token to the next node. The token passing scheme is efficient compared to the polling technique, but it relies on the correct and reliable operation of all the nodes. There

exists a number of potential problems, such as lost token, duplicate token, and insertion of a node, removal of a node, which must be tackled for correct and reliable operation of this scheme.

- Performance of a token ring network can be represented by two parameters; throughput, which is a measure of the successful traffic, and delay, which is a measure of time between when a packet is ready and when it is delivered.



Token ring network

❖ Contention-based Approaches

- Round-Robin techniques work efficiently when majority of the stations have data to send most of the time. But, in situations where only a few nodes have data to send for brief periods of time, Round-Robin techniques are unsuitable.
- Contention techniques are suitable for bursty nature of traffic. In contention techniques, there is no centralized control and when a node has data to send, it contends for gaining control of the medium.
- The principle advantage of contention techniques is their simplicity.
- They can be easily implemented in each node.
- The techniques work efficiently under light to moderate load,
- But performance rapidly falls under heavy load.

(2) Carrier Sense Multiple Access (CSMA):

Procedure

- Listen to medium and wait until it is free (no one else is talking)
- Wait a random back off time then start talking

Advantages

- Fairly simple to implement
- Functional scheme that works

Disadvantages

- Can not recover from a collision

  (Inefficient waste of medium time)

(3) Carrier Sense Multiple Access with Collision Detection (CSMA-CD):

- This refined scheme is known as Carrier Sensed Multiple Access with Collision Detection (CSMA/CD) or Listen-While-Talk.
- CSMA/CD protocol can be considered as a refinement over the CSMA scheme.

Procedure

- Listen to medium and wait until it is free
- Then start talking, but listen to see if someone else starts talking too
- If a collision occurs, stop and then start talking after a random back off time
- This scheme is used for hub based Ethernet

Advantages

- More efficient than basic CSMA

Disadvantages

- Requires ability to detect collisions.

(4) Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) :

Procedure

- Similar to CSMA but instead of sending packets control frames are exchanged
- RTS = request to send
- CTS = clear to send
- DATA = actual packet
- ACK = acknowledgement

Advantages

- Small control frames lessen the cost of collisions (when data is large)
- RTS + CTS provide “virtual” carrier sense which protects against hidden terminal collisions (where A can’t hear B)

Disadvantages:

- Not as efficient as CSMA-CD
- Doesn’t solve all the problems of MAC in wireless networks (more to come)

❖ **COMMUNICATION METHODS:-**

→ **Unicast**

- 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.

→ **Broadcast**

- 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).

→ **Multicast**

- 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 (theer 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 salability 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.
- The multicast mode is useful if a group of clients require a common set of data at the same time, or when the clients are able to receive and store (cache) common data until needed. Where there is a common need for the same data required by a group of clients, multicast transmission may provide significant bandwidth savings (up to 1/N of the bandwidth compared to N separate unicast clients).
- The majority of installed LANs (e.g. Ethernet) are able to support the multicast transmission mode. Shared LANs (using hubs/repeaters) inherently support multicast, since all packets reach all network interface cards connected to the LAN. The earliest LAN network interface cards had no specific support for multicast and introduced a big performance penalty by forcing the adaptor to receive all packets (promiscuous mode) and perform software filtering to remove all unwanted packets. Most modern network interface cards implement a set of multicast filters, relieving the host of the burden of performing excessive software filtering.

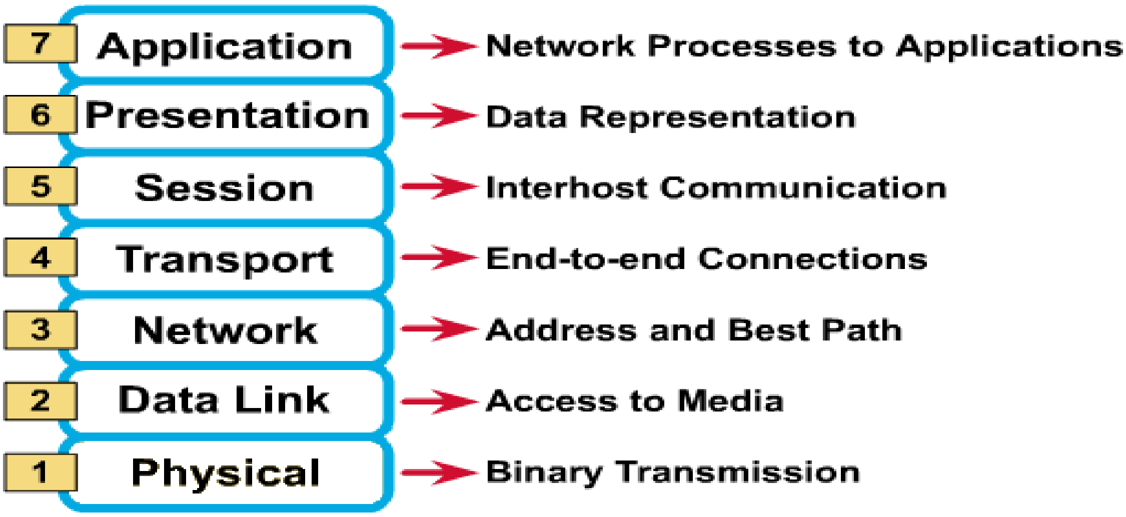
Chapter 2: Network Standards

❖ Open Systems Interconnection (OSI) Model :

- International standard organization (ISO) established a committee in 1977 to develop architecture for computer communication.
- Open Systems Interconnection (OSI) reference model is the result of this effort.

- In 1984, the Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture.
- Term "open" denotes the ability to connect any two systems which conform to the reference model and associated standards.
- The OSI model is now considered the primary Architectural model for inter-computer communications.
- The OSI model describes how information or data makes its way from application programmes (such as spreadsheets) through a network medium (such as wire) to another application programme located on another network.
- The OSI reference model divides the problem of moving information between computers over a network medium into SEVEN smaller and more manageable problems.
- This separation into smaller more manageable functions is known as layering.

OSI Reference Model: 7 Layers


7 Application → Network Processes to Applications
6 Presentation → Data Representation
5 Session → Interhost Communication
4 Transport → End-to-end Connections
3 Network → Address and Best Path
2 Data Link → Access to Media
1 Physical → Binary Transmission

➢ **Physical Layer :**

- Provides physical interface for transmission of information.
- Defines rules by which bits are passed from one system to another on a physical communication medium.
- Covers all - mechanical, electrical, functional and procedural - aspects for physical communication.
- Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes are defined by physical layer specifications.

➢ **Data Link Layer :**

- Data link layer attempts to provide reliable communication over the physical layer interface.
- Breaks the outgoing data into frames and reassemble the received frames.
- Create and detect frame boundaries.
- Handle errors by implementing an acknowledgement and retransmission scheme.
- Implement flow control.
- Supports points-to-point as well as broadcast communication.

- Supports simplex, half-duplex or full-duplex communication.

➢ **Network Layer :**

- Implements routing of frames (packets) through the network.
- Defines the most optimum path the packet should take from the source to the destination
- Defines logical addressing so that any endpoint can be identified.
- Handles congestion in the network.
- Facilitates interconnection between heterogeneous networks (Internetworking).
- The network layer also defines how to fragment a packet into smaller packets to accommodate different media.

➢ **Transport Layer :**

- Purpose of this layer is to provide a reliable mechanism for the exchange of data between two processes in different computers.
- Ensures that the data units are delivered error free.
- Ensures that data units are delivered in sequence.
- Ensures that there is no loss or duplication of data units.
- Provides connectionless or connection oriented service.
- Provides for the connection management.
- Multiplex multiple connections over a single channel.

➢ **Session Layer :**

- Session layer provides mechanism for controlling the dialogue between the two end systems. It defines how to start, control and end conversations (called sessions) between applications.
- This layer requests for a logical connection to be established on an end-user's request.
- Any necessary log-on or password validation is also handled by this layer.
- Session layer is also responsible for terminating the connection.
- This layer provides services like dialogue discipline which can be full duplex or half duplex.
- Session layer can also provide check-pointing mechanism such that if a failure of some sort occurs between checkpoints, all data can be retransmitted from the last checkpoint.

➢ **Presentation Layer :**

- Presentation layer defines the format in which the data is to be exchanged between the two communicating entities.
- Also handles data compression and data encryption (cryptography).

➢ **Application Layer :**

- Application layer interacts with application programs and is the highest level of OSI model.
- Application layer contains management functions to support distributed applications.
- Examples of application layer are applications such as file transfer, electronic mail, remote login etc.

❖ **ENCRYPTION**:-

→ In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor.

→ In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read 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, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors.

❖ **COMPRESSION**:-

→ In digital signal processing, data compression, source coding, or bit-rate reduction involves encoding information using fewer bits than the original representation. Compression can be either lossy or lossless.

→ Lossless compression reduces bits by identifying and eliminating statistical redundancy. No information is lost in lossless compression. Lossy compression reduces bits by identifying unnecessary information and removing it.The process of reducing the size of a data file is referred to as data compression.

→ In the context of data transmission, it is called source coding (encoding done at the source of the data before it is stored or transmitted) in opposition to channel coding.

→ Compression is useful because it helps reduce resource usage, such as data storage space or transmission capacity. Because compressed data must be decompressed to use, this extra processing imposes computational or other costs through decompression; this situation is far from being a free lunch.

→ Data compression is subject to a space–time complexity trade-off. For instance, a compression scheme for video may require expensive hardware for the video to be decompressed fast enough to be viewed as it is being decompressed, and the option to decompress the video in full before watching it may be inconvenient or require additional storage.

→ The design of data compression schemes involves trade-offs among various factors, including the degree of compression, the amount of distortion introduced (when using lossy data compression), and the computational resources required to compress and decompress the data.

❖ **DISK QUOTA:-**

→ A disk quota is a limit set by a system administrator that restricts certain aspects of file system usage on modern operating systems. The function of using disk quotas is to allocate limited disk space in a reasonable way.

→ Types of quotas:-

- There are two basic types of disk quotas. The first, known as a *usage quota* or *block quota*, limits the amount of disk space that can be used. The second, known as a *file quota* or *inode quota*, limits the number of files and directories that can be created.
- In addition, administrators usually define a warning level, or *soft quota*, at which users are informed they are nearing their limit, that is less than the effective limit, or *hard quota*. There may also be a small *grace interval*, which allows users to temporarily violate their quotas by certain amounts if necessary.

❖ **MAPPING NETWORK DRIVE:-**

→ Drive mapping is how operating systems, such as Microsoft Windows, associate a local drive letter (A through Z) with a shared storage area to another computer over a network.

→ After a drive has been mapped, a software application on a client's computer can read and write files from the shared storage area by accessing that drive, just as if that drive represented a local physical hard disk drive.

Drive Mapping

- → Mapped Drives are hard drives (even if located on a virtual or cloud computing system, or network drives) which are always represented by names, letter(s), or number(s) and they are often followed by additional strings of data, directory tree branches, or alternate level(s) separated by a "\" symbol.
- → Drive mapping is used to locate directories, files or objects, and programs or apps, and is needed by end users, administrators, various other operators, and users or groups.
- → Mapped drives are usually assigned a letter of the alphabet after the first few taken, such as A:\, B:\, C:\, and D:\ (which is usually an optical drive unit). Then, with the drive and/or directory (letters, symbols, numbers, names, and all other components) to be mapped and might be entered into the necessary address bar/location(s).

❖ **NETMEETING** :-

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

❖ **FILE AND PRINT SERVICE:-**

File and printer sharing, information retrieval, and data storage are among the most frequently used network services. They are therefore crucial factors to consider when choosing a network operating system.

- → Microsoft built the Windows® 2000 Server operating system from the ground up as an integrated, multipurpose operating system. The operating system design responds to customer demands for sophisticated but easy-to-manage file and print services, for integration of Web and media content with file and print information sharing, and for meeting exponential growth in storage requirements while lowering storage cost. In addition, its open architecture lets third-party developers provide additional functionality in response to ever-changing business requirements.

→ Microsoft developed specific file and print features to meet widespread customer needs:

- **Reduced cost.** Remote Storage migrates infrequently used files to lower-cost secondary storage, yet keeps that data available if needed. Removable Storage helps reduce costs by letting multiple client applications share local libraries and tape or disk drives while ensuring that client applications do not corrupt each other's data.
- **Better manageability.** The improved NTFS file system, distributed file system (Dfs), and Indexing Service make it easier to find and access files across expanding networks. New interfaces make operating system services easier to manage; for example, the new printer interface makes it simpler for both administrators and end-users to configure and manage their printing needs.

- **Increased availability and reliability.** Dfs replication and File Replication service (FRS) synchronization help keep data available to users, even if a server or disk drive fails or a shared folder or file becomes corrupted. Dynamic volumes formatted with NTFS 5 allow fewer reboots when adding disks and creating, extending, or mirroring a volume.
- **Scalability.** The Windows 2000 NTFS version 5 file system and the Windows 2000 storage subsystems let users efficiently store and retrieve ever-larger quantities of data.

→ Organizations that install Windows 2000 file and print servers in their existing network c can take advantage of several new features. When they upgrade to a Windows 2000 network, additional file and print capabilities become available.

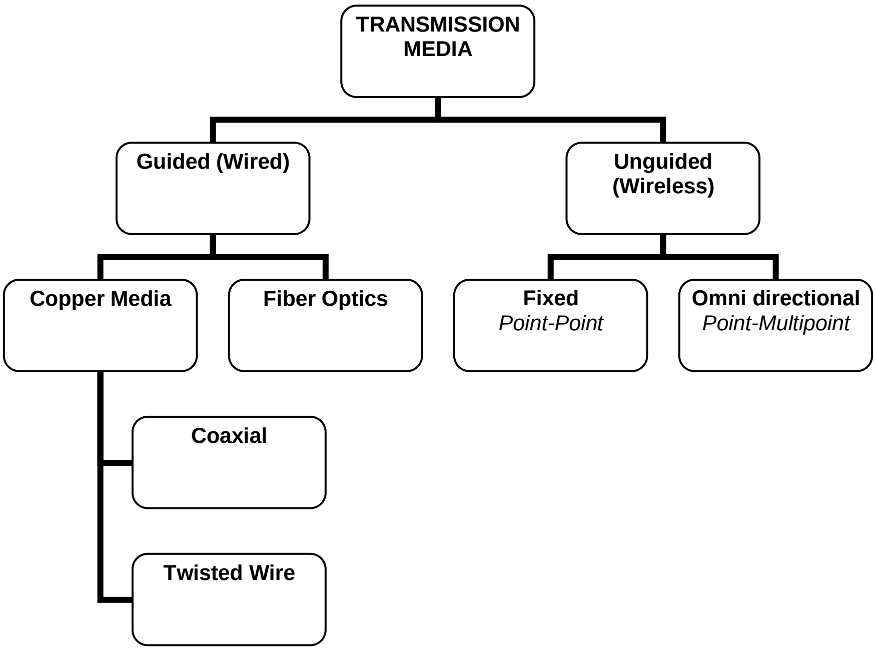
→ This overview focuses primarily on the Windows 2000 Server implementation of the standard file and print services components. However, it includes mention of several Web-related features where they are inextricably bound up with file and print services.

UNIT 2

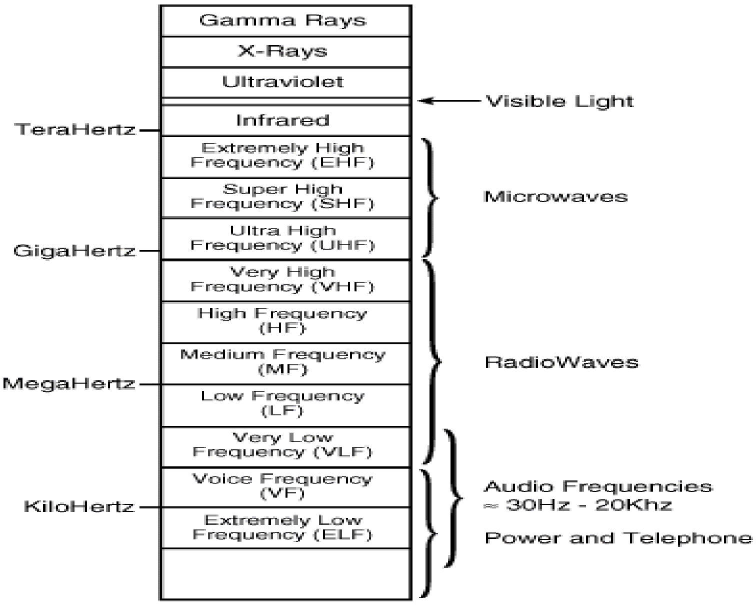
Transmission Media

❖ Types of Transmission Media :

- Transmission media is divided into two: Wired or Wireless
- **Wired Media** is the most common and is further divided into three different types of cabling: Coaxial, Twisted Pairs, and Fiber Optic Cables
- **Wireless media**, which is, in a sense, no media at all, is also gaining popularity. Wireless transmissions use radio waves or infrared light to transmit data.



❖ TRANSMISSION FREQUENCIES



2GHz to 40GHz

- Microwave
- Highly directional

  Point to point

  Satellite

30MHz to 1GHz

- Omni directional
- Broadcast radio

3 x 1011 to 2 x 1014

- Infrared
- Local

❖ CHARACTERISTICS OF TRANSMISSION MEDIA:

Each type of transmission media has special listed as follows:

- Cost
- Installation requirements
- Bandwidth
- Band Usage (Baseband or Broadband)
- Attenuation
- Immunity from electromagnetic interference

Bandwidth

- The term Bandwidth refers to the measure of the capacity of a medium to transmit data.
- Data transmission rates frequently are stated in terms of the bits that can be transmitted per second. The bandwidth that a cable can accommodate is determined in part by the cable’s length. A short cable generally can accommodate greater bandwidth than a long cable.

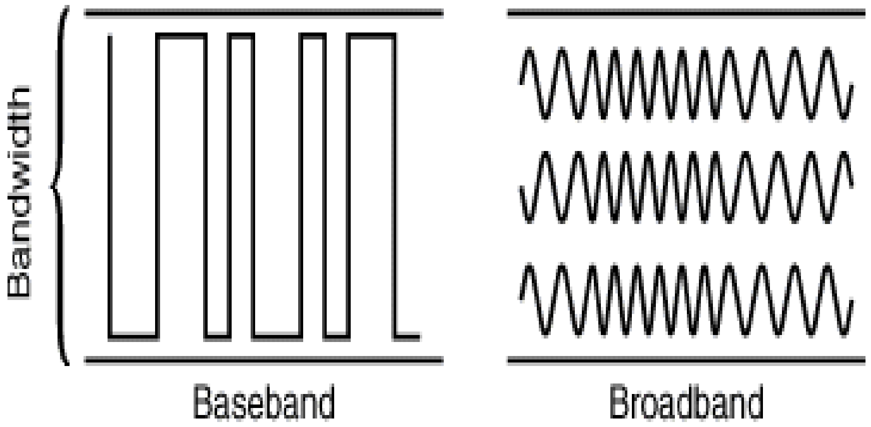
➢ **Band Usage**

- Band Usage is the allocation of the capacity of transmission media and has two ways: **baseband** and **broadband** transmissions.

➢ **Baseband**

- Baseband is the most common mode of operation and devotes the entire capacity of the medium to one communication channel. Baseband signaling can be accomplished with both analog and digital signals

- **Broadband**
- Broadband enables two or more communication channels to share the bandwidth of the communications medium. This technique of dividing bandwidth into frequency bands is called frequency-division multiplexing (FDM) and works only with analog signals. Another technique, called time-division multiplexing (TDM), supports digital signals.



- **Attenuation**
- Attenuation is a measure of how much a signal weakens as it travels through a medium.
- **Electromagnetic interference (EMI)** consists of outside electromagnetic noise that distorts the signal in a medium. EMI in the form of noise caused by nearby motors or lightning. Some network media are more susceptible to EMI than others.
- **Crosstalk** is a special kind of interference caused by adjacent wires. Crosstalk is a particularly significant problem because large numbers of cables often are located close together with minimal attention to exact placement.

❖ GUIDED TRANSMISSION MEDIA (CABLE):

- Guided Transmission Media uses a **cabling** system that guides the data signals along a **specific path**.
- Guided Media is also known as **Bounded Media**, since the data signals are a bounded system.
- Cabling technology is not limited to copper wire only. Cables can be any physical or conductive media like **wires**, **coaxial cables** or **fibre optics**
- **COAXIAL CABLE :**
- Coaxial cables were the first cable types used in communications technology.
- It consists of two conductors that share a common axis
- **The components of a coaxial cable are as follows:**
- Center conductor
- Outer conductor
- Insulation layer

- Plastic encasement/jacket

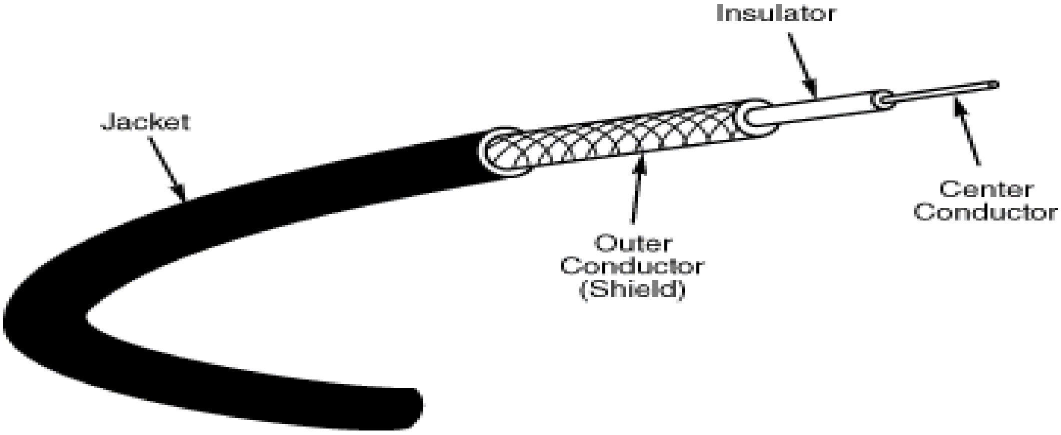


Fig: Coaxial Cable

- **Types of Coaxial Cable**
- **Thinnet:** is a light and flexible cabling medium that is inexpensive and easy to install.
- **Thicknet:** is thicker and does not bend as readily as Thinnet, Thicknet cable is harder to work with. A thicker center core, however, means that Thicknet can carry more signals a longer distance than Thinnet.
- **Coaxial Characteristics**
- **Installation**
- Coaxial cable is reasonably easy to install because the cable is strong and difficult to break. In addition, connectors can be installed with inexpensive tools and a bit of practice. The device-to-device cabling approach can be difficult to reconfigure, however, when new devices cannot be installed near an existing cabling path.
- **Cost**
- The coaxial cable used for Thinnet falls at the low end of the cost spectrum, whereas Thicknet is among the more costly options.
- **Bandwidth**
- Computes that employ coaxial cable typically have a bandwidth between 2.5 Mbps and 10 Mbps. Thicker coaxial cables offer higher bandwidth, and the potential bandwidth of coaxial is much higher than 10 Mbps.
- **EMI Characteristics**
- All copper media are sensitive to EMI, although the shield in coax makes the cable fairly resistant. Coaxial cables, however, do radiate a portion of their signal, and electronic eavesdropping equipment can detect this radiated signal.
- **Coaxial Application**
- Most versatile medium
- Television distribution
- Long distance telephone transmission
- Short distance computer systems links
- Local area networks

❖ TWISTED PAIR CABLE :

- A basic **twisted-pair cable** consists of two strands of copper wire twisted together.
- This twisting reduces the sensitivity of the cable to EMI and also reduces the tendency of the cable to radiate radio frequency noise that interferes with nearby cables and electronic components.
- Twisted-pair cable is inexpensive to install.

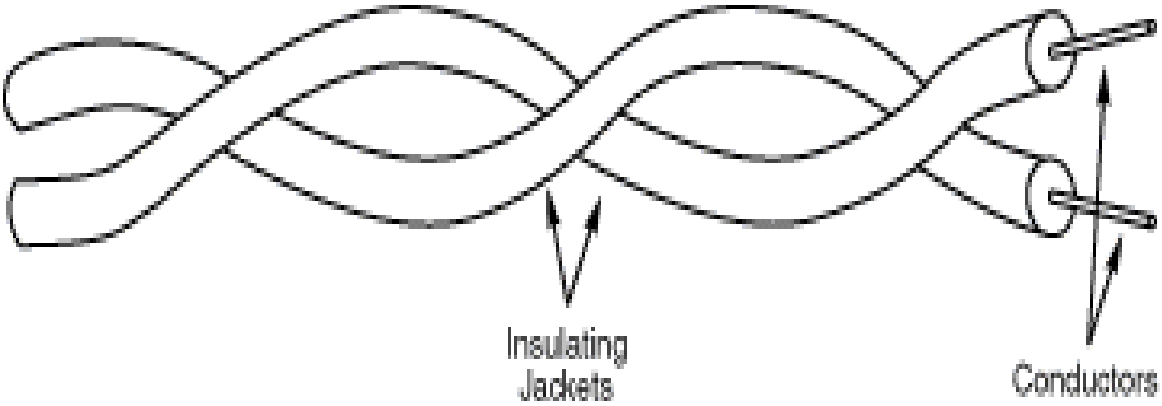
- Offers the lowest cost per foot of any cable type.

Application:

- Most common medium
- Telephone network
  - — Between house and local exchange (subscriber loop)
- Within buildings
  - — To private branch exchange (PBX)
- For local area networks (LAN)
  - — 10Mbps or 100Mbps

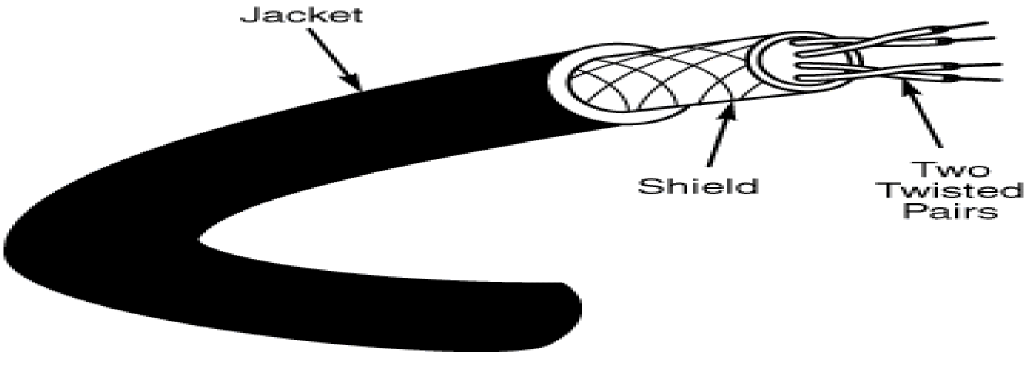
Twisted Pair Cable

- Two types of twisted-pair cable are used: (1) shielded and (2) unshielded.



(1) SHIELDED TWISTED PAIR CABLE:

- Shielded twisted-pair cabling consists of one or more twisted pairs of cables enclosed in a foil wrap and woven copper shielding.
- Metal braid or sheathing that reduces interference
- More expensive
- Harder to handle (thick, heavy)



STP Characteristics

- **Installation**
- Naturally, different network types have different installation requirements. One major difference is the connector used. In many cases, installation can be greatly simplified by using pre-wired cables.
- **Cost**
- STP cable costs more than thin coaxial or unshielded twisted-pair cable. STP is less costly, however, than thick coax or fiber-optic cable.
- **Capacity**
- The most common data rate for STP cable is 16 Mbps, which is the top data rate for Token Ring networks.
- **Attenuation**

- All varieties of twisted-pair cable have attenuation characteristics that limit the length of cable runs to a few hundred meters, although a 100-meter limit is most common.
- **EMI Characteristics**
- The shield in STP cable results in good EMI characteristics for copper cable. Comparable to the all copper cables, STP is sensitive to interference and vulnerable to electronic eavesdropping.

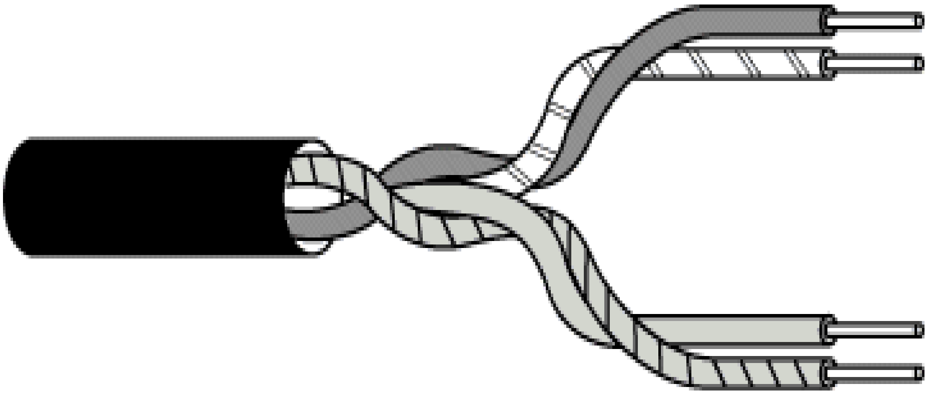
(2) UNSHIELDED TWISTED PAIR CABLE:

- The characteristics of the **Unshielded Twisted Pair cables (UTP)** are similar in many ways to STP, differing primarily in attenuation and EMI. Several twisted-pairs can be bundled together in a single cable. These pairs typically are color coded to distinguish them.
- Ordinary telephone wire
- Cheapest
- Easiest to install
- Suffers from external EM interference

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

- **Categories 1 and 2** - voice-grade cables are suitable only for voice and for low data rates (below 4 Mbps)
- **Category 3** - generally suited for data rates up to 10 Mbps
- **Category 4** - consists of four twisted-pairs, is suitable for data rates up to 16 Mbps.
- **Category 5** - consists of four twisted-pairs, is suitable for data rates up to 100 Mbps.

UNSHIELDED TWISTED PAIR CABLE

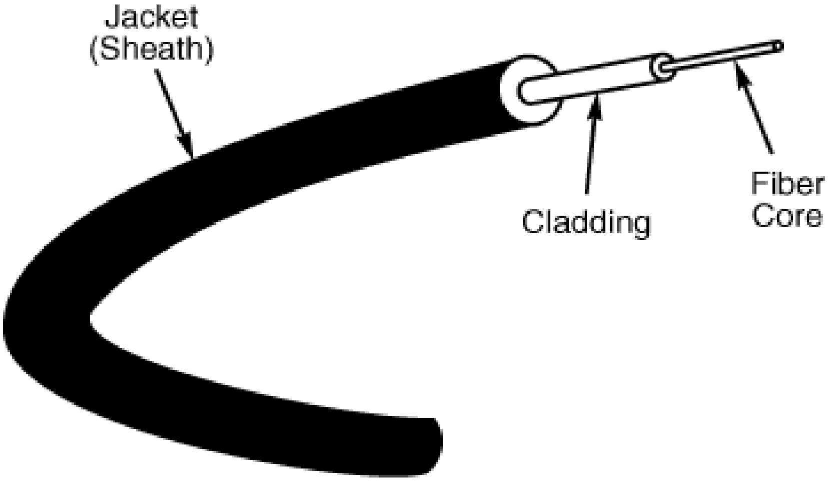


- **UTP Characteristics**
- **Installation**
- UTP cable is easy to install. Some specialized equipment might be required, but the equipment is low in cost.
- Category 5 cable has stricter installation requirements than lower categories of UTP.
- **Cost**
- UTP cable is the less costly, although properly installed Category 5 tends to be fairly expensive. Distance limits for voice cabling are much less severe than for data-grade cabling.
- **Capacity**
- The data rates possible with UTP have pushed up from 1 Mbps, past 4 and 16 Mbps, to the point where 100 Mbps data rates are now common.
- **Attenuation**

- UTP cable shares similar attenuation characteristics with other copper cables. UTP cable runs are limited to a few hundred meters, with 100 meters as the most frequent limit.
- **EMI Characteristics**
- Because UTP cable lacks a shield, it is more sensitive to EMI than coaxial or STP cables. UTP might not be suitable for noisy environments such as factories. Crosstalk between nearby unshielded pairs limits the maximum length of cable runs

❖ FIBER-OPTIC CABLE :

- Fiber-optic cable is the ideal cable for data transmission because it accommodates extremely high bandwidths,
- has no problems with EMI, ssupports durable cables and cable runs as long as several kilometers.
- The two disadvantages of fiber-optic, however, are cost and installation difficulty.
- Optical fiber cables don’t transmit electrical signals. Instead, the data signals must be converted into light signals.



Fiber Optic Cable

- The center conductor of a fiber-optic cable is a fiber that consists of highly refined glass or plastic. The fiber is coated with a cladding that reflects signals back into the fiber to reduce signal loss. A plastic sheath protects the fiber.
- A fiber-optic network cable consists of two strands separately enclosed in plastic sheaths—one strand sends and the other receives.
- Two types of cable configurations are available: loose and tight configurations.
- **Application :**
- greater capacity (bandwidth of up to 2 Gbps)
- smaller size and lighter weight
- lower attenuation
- immunity to environmental interference
- highly secure due to tap difficulty and lack of signal radiation
- **Fiber-Optics Characteristics**
- **Installation**
- Fiber-optic cable requires greater care because the cables must be treated fairly gently during installation. Every cable has a minimum bend radius, and fibers are damaged if the cables are bent too sharply. It also is important not to stretch the cable during installation.
- **Cost**
- Fiber-optic cable is the most expensive cable type to install.

- **Capacity**
- Fiber-optic cable can support high data rates (as high as 200,000 Mbps) even with long cable runs. Fiber-optic cables can transmit 100 Mbps signals for several kilometers.
- **Attenuation**
- Attenuation in fiber-optic cables is much lower than in copper cables. Fiber-optic cables are capable of carrying signals for several kilometers.
- **EMI Characteristics**
- Because fiber-optic cables don't use electrical signals to transmit data, they are totally immune to electromagnetic interference. The cables also are immune to a variety of electrical effects that must be taken into account when designing copper cabling systems.
- Because the signals in fiber-optic cable are not electrical in nature, they cannot be detected by the electronic eavesdropping equipment that detects electromagnetic radiation. Therefore, fiber-optic cable is the perfect choice for high-security networks.

❖ **UNGUIDED TRANSMISSION MEDIA (Wireless):**

- **Unguided Media or Wireless Communication** consists of a means (e.g. air, space) for the data signals to travel, where there is nothing to guide them along a specific path, like in wires.
- Unbounded media is electromagnetic waves in form of radio, microwave, infrared or others.
- Wireless communication is used where cables are difficult to use or install.
- Wireless transmission media refers to the methods of carrying data through the air or space using infrared, radio, or microwave signals.

● **REASONS FOR WIRELESS TECHNOLOGY:**

- Spaces where cabling would be impossible or inconvenient.
- People who move around a lot within their work environment.
- Temporary installations.
- People who travel outside of the work environment and need instantaneous access to network resources.

● **CLASSIFICATIONS OF WIRELESS TRANSMISSION:**

- **Classification by Propagation :**
- Fixed (Directional)
- Mobile (Omni directional)
- **Classification by Method**
- Infrared
- Laser
- Narrow-band radio
- Spread-spectrum radio
- Microwaves

➢ **Infrared :**

- Infrared is a wireless transmission medium that carries data via light beams.
- Transmitter and receiver must be in line of sight.
- Infrared technology allows computing devices to communicate via short-range wireless signals using infrared lights wherein they are typically are limited to within 100 feet.

- Uses transmitters/receivers (transceivers) that modulate no coherent infrared light.
- Transceivers must be within line of sight of each other (directly or via reflection).
- Unlike microwaves, infrared does not penetrate walls.
- Initially used in remote controls
- **Advantages:**
- Portable - no antennae required
- Inexpensive
- **Disadvantages:**
- Limited range
- Very Sensitive

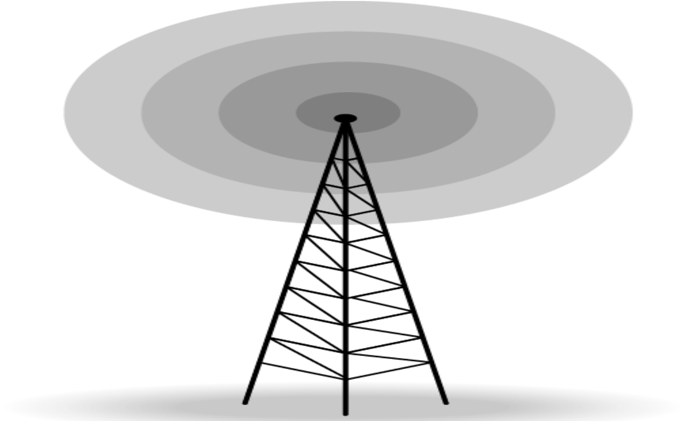
➢ **Laser Transmission :**

- High-powered laser transmitters can transmit data for several thousand yards when line-of-sight communication is possible.
- Lasers can be used in many of the same situations as microwave links
- Laser light technology is similar to infrared technology.

➢ **Radio :**

- I Radio is a wireless transmission medium that carries data via radio frequency signals.
- Wireless LANs in a home or business are one type of radio technology.
- Radio signals can be long range (between cities or regions) and short range (within a building).
- Radio signals are susceptible to noise and electrical Interference.
- Radio waves are used for multicast communications,
- such as radio and television, and paging systems.
- They can penetrate through walls.
- Highly regulated.
- Use Omni directional antennas
- Radio is a general term often used to encompass frequencies in the range 3 kHz to 300 GHz.

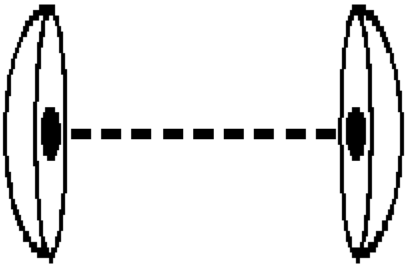
Omni directional antenna



➢ **Microwaves :**

- Microwaves are high frequency radio waves.
- Much of long-distance telephone service is carried by microwaves.
- Microwaves travel in a straight line.
- Microwave relay stations are built about 30 miles apart.
- Microwaves are used for unicast communication.
- Such as cellular telephones, satellite networks, and wireless LANs.
- Higher frequency ranges cannot penetrate walls.
- Use directional antennas - point to point line of sight communications

Directional Point-to-point focused beams employing high frequencies



Applications:

- Television distribution
- Long-distance telephone transmission
- Private business networks

Disadvantages:

- Line of sight requirement
- Expensive towers and repeaters
- Subject to interference such as passing airplanes and rain

❖ The Concept of Multiplexing:

- **Multiplexing** refers to the combination of information streams from multiple sources for transmission over a shared medium.
- **Demultiplexing** refers to the separation of a combination of information streams back into separate information streams

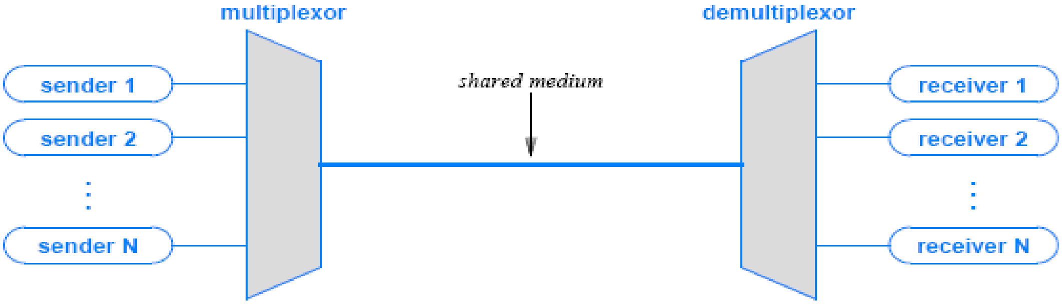
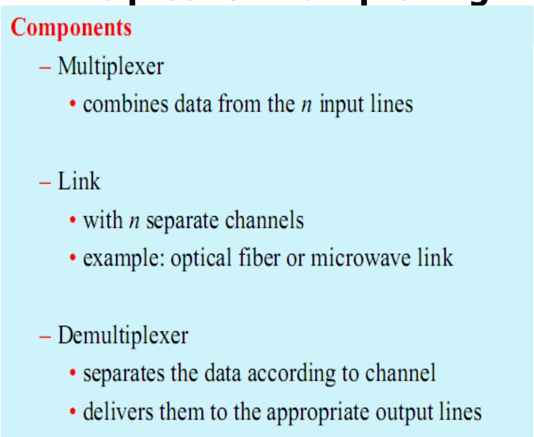


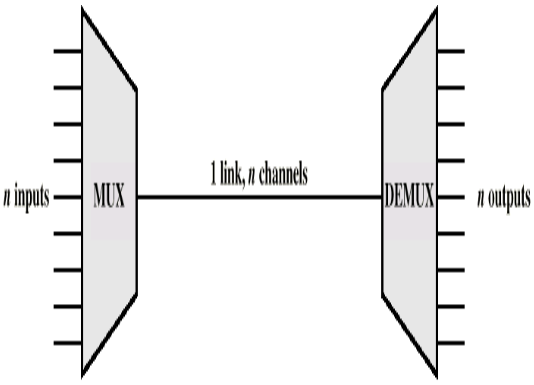
Figure 11.1 The concept of multiplexing in which independent pairs of senders and receivers share a transmission medium.

❖ Principles of Multiplexing:



Components

- Multiplexer
  - combines data from the *n* input lines
- Link
  - with *n* separate channels
  - example: optical fiber or microwave link
- Demultiplexer
  - separates the data according to channel
  - delivers them to the appropriate output lines



- **Multiplexing : Applications:**

- Telephone systems
- Telemetry
- Satellites
- Broadcasting (radio and TV)

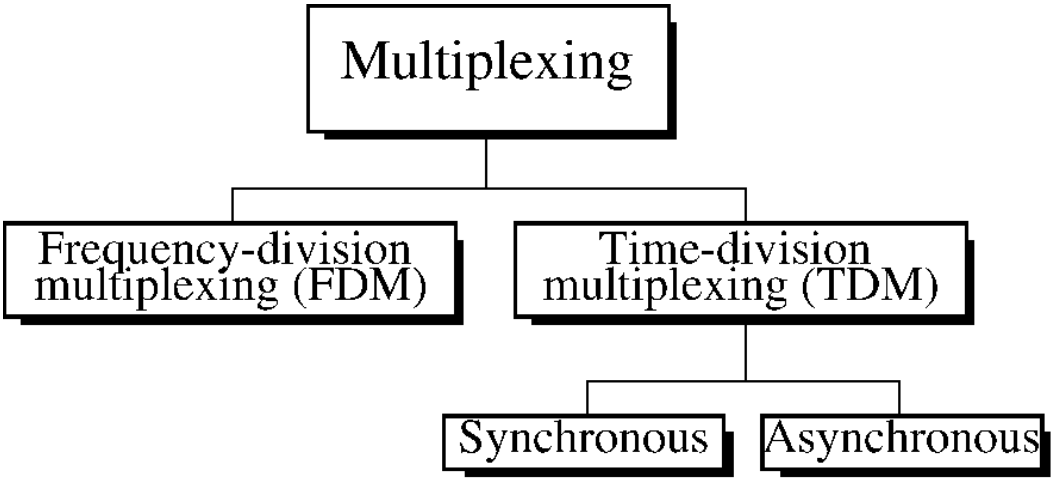
Basic Types of Multiplexing:

- There are four basic approaches to multiplexing that each have a set of variations and implementations
  1. Frequency Division Multiplexing (FDM)
  2. Wavelength Division Multiplexing (WDM)
  3. Time Division Multiplexing (TDM)
  4. Code Division Multiplexing (CDM)
- TDM and FDM are widely used
- WDM is a form of FDM used for optical fiber
- CDM is a mathematical approach used in cell phone mechanisms.

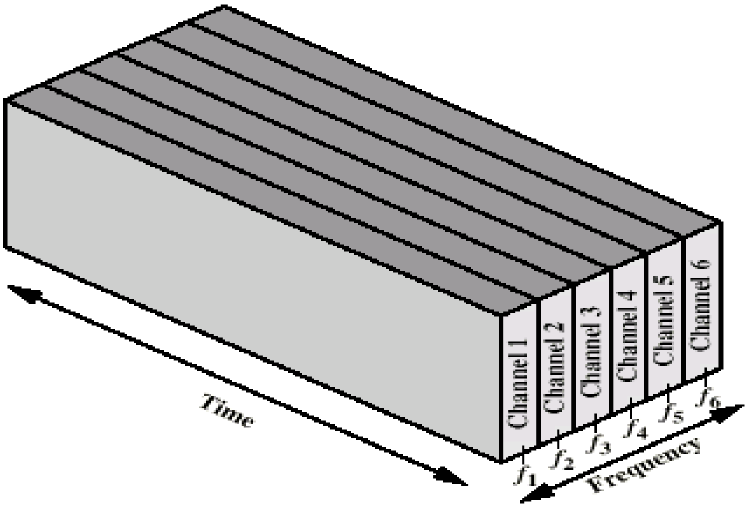
The two most common types of multiplexing are :

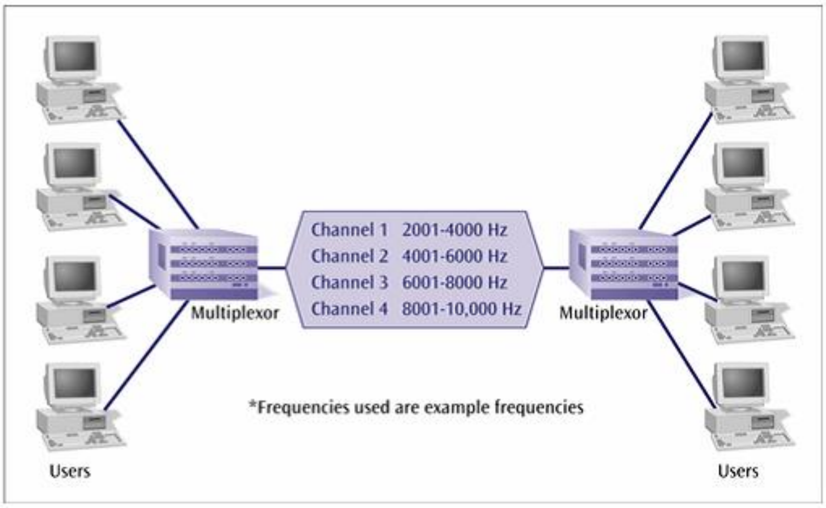
1. Frequency-division multiplexing (FDM)
   - Generally used for analog information.
   - Individual signals to be transmitted are assigned a different frequency within a common bandwidth.
2. Time-division multiplexing (TDM)
   - Generally used for digital information.
   - Multiple signals are transmitted in different time slots on a single channel.

➢ **Types of multiplexing:-**


Multiplexing
Frequency-division multiplexing (FDM)
Time-division multiplexing (TDM)
Synchronous
Asynchronous

FrequencyDivisionMultiplexing(FDM) :





FDM: all signals are transmitted at the same time (all the time) but in different frequency bands

- It is possible to send Simultaneously multiple carrier waves over a single copper wire
- A demultiplexor applies a set of filters that each extract a small range of frequencies near one of the carrier frequencies.
- Advantage of FDM arises from the simultaneous use of a transmission medium by multiple pairs of entities
- We imagine FDM as providing each pair with a private transmission path
- as if the pair had a separate physical transmission medium

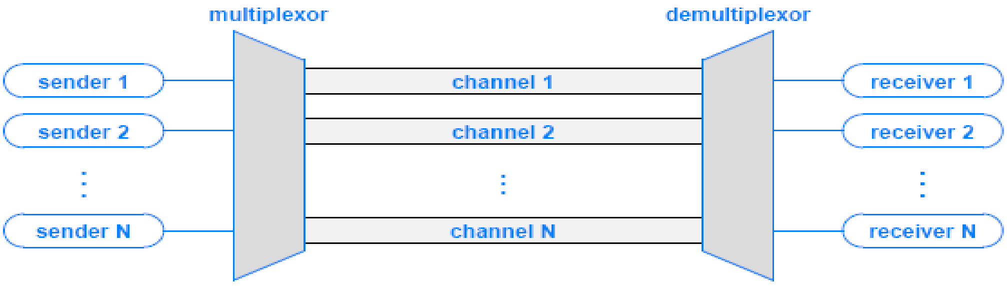
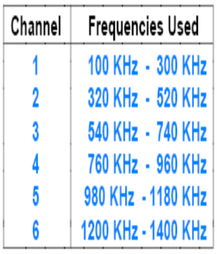


Figure 11.3 The conceptual view of Frequency Division Multiplexing (FDM) as providing a set of independent channels.

- **Limitations Of FDM :**

  In practical FDM systems, there are some limitations:

  - If the frequencies of two channels are too close, interference can occur
  - Furthermore, demultiplexing hardware that receives a combined signal must be able to divide the signal into separate carriers
  - Designers choosing a set of carrier frequencies with a gap between them known as a guard band



Channel	Frequencies Used
1	100 KHz - 300 KHz
2	320 KHz - 520 KHz
3	540 KHz - 740 KHz
4	760 KHz - 960 KHz
5	980 KHz - 1180 KHz
6	1200 KHz - 1400 KHz

Figure 11.4 An example assignment of frequencies to channels with a guard band between adjacent channels.

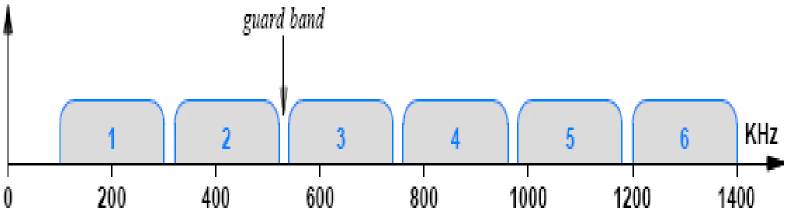


Figure 11.5 A frequency domain plot of the channel allocation from Figure 11.4 with a guard band visible between channels.

- **FDM Advantages & Disadvantages :**

  Advantages:

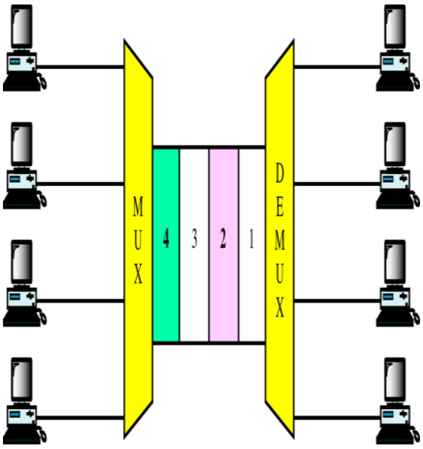
  – no dynamic coordination needed

  Disadvantages:

  – guard spaces

❖ Time Division Multiplexing(TDM):

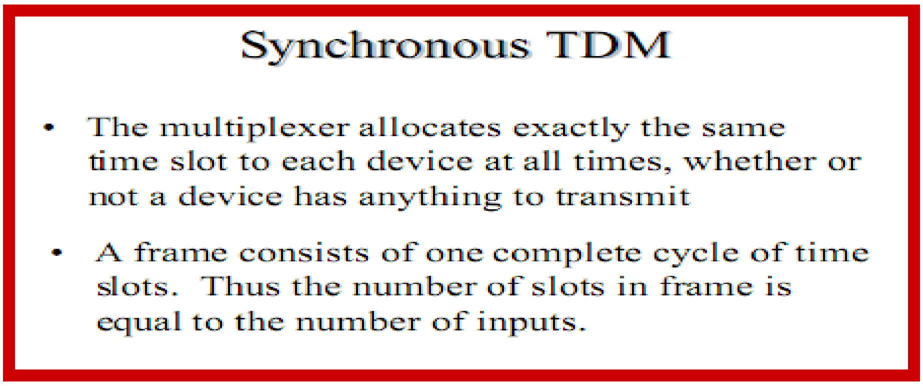
- Generally used for digital information.
- Multiple signals are transmitted in different time slots on a single channel.



- Sharing of the signal is accomplished by dividing available transmission time on a medium among users.
- Digital signaling is used exclusively.
- Time division multiplexing comes in two basic forms:
  - Synchronous time division multiplexing, and
  - Statistical, or asynchronous time division multiplexing.

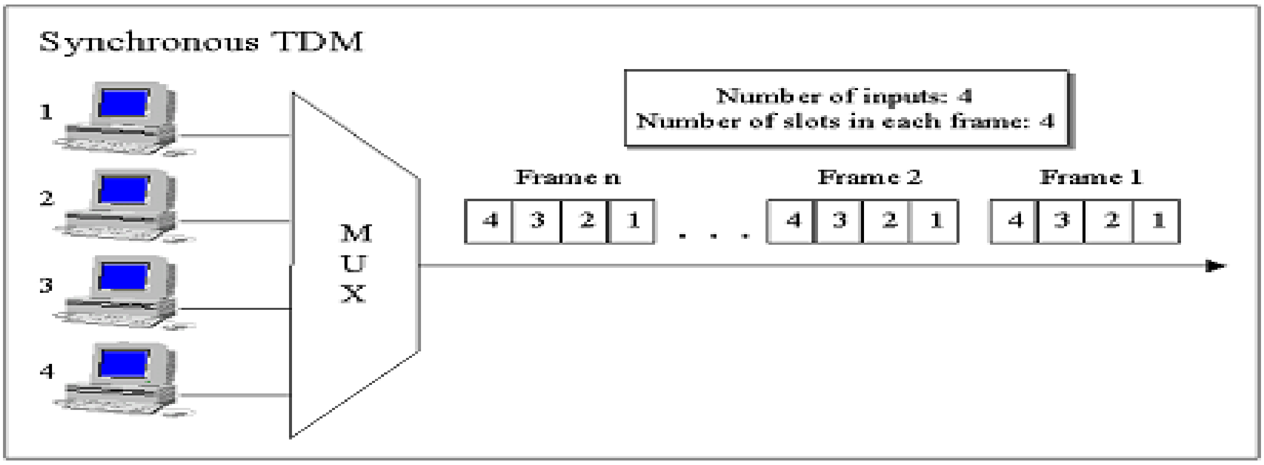
❖ Synchronous TDM :

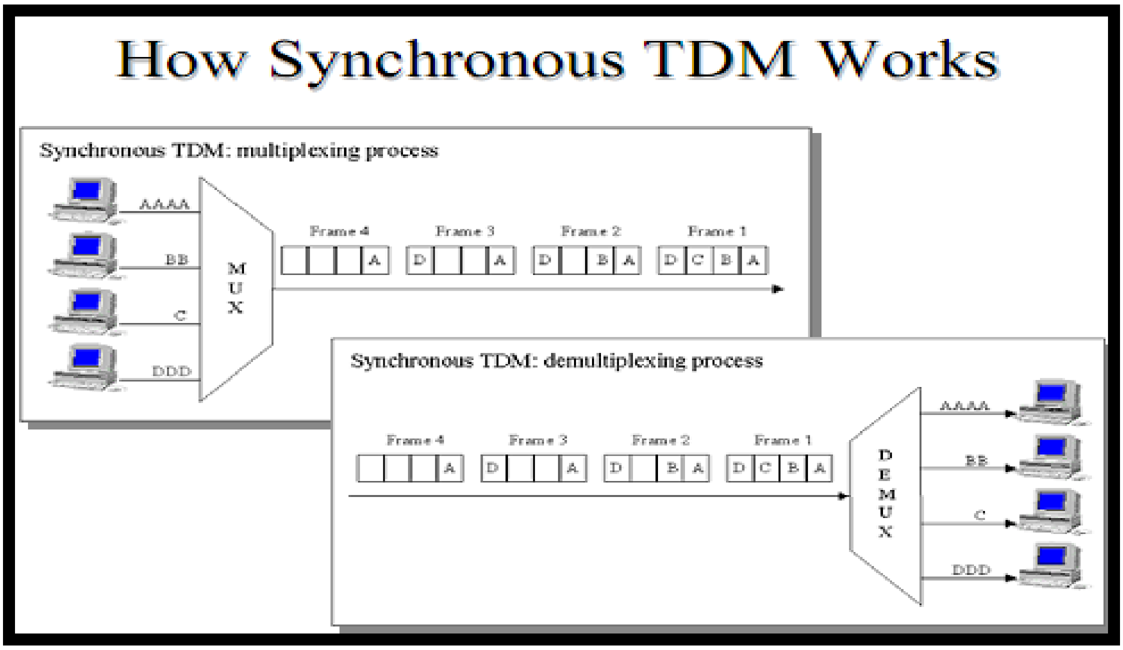
- It is widely used throughout the Internet



Synchronous TDM

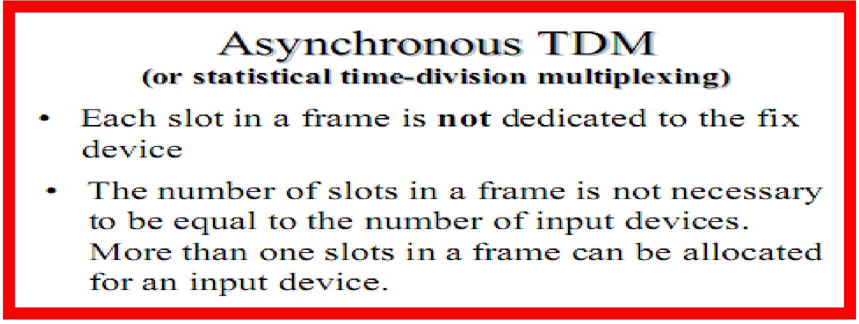
- The multiplexer allocates exactly the same time slot to each device at all times, whether or not a device has anything to transmit
- A frame consists of one complete cycle of time slots. Thus the number of slots in frame is equal to the number of inputs.





How Synchronous TDM Works

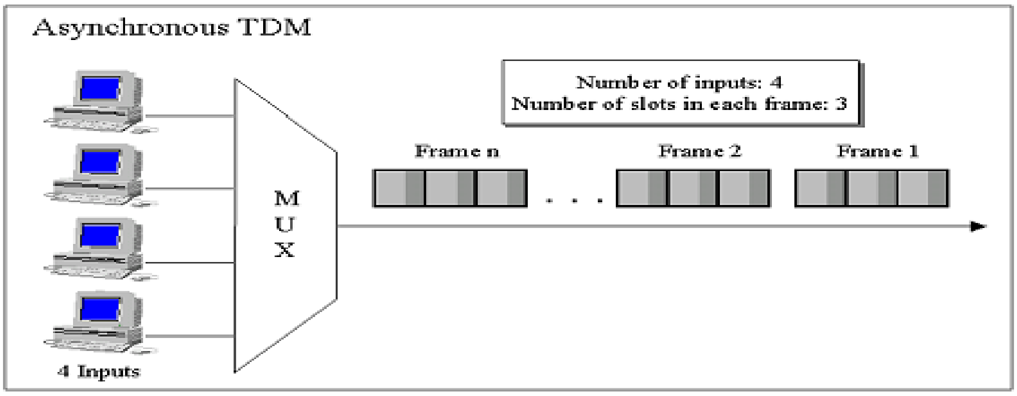
❖ **Asynchronous TDM :**

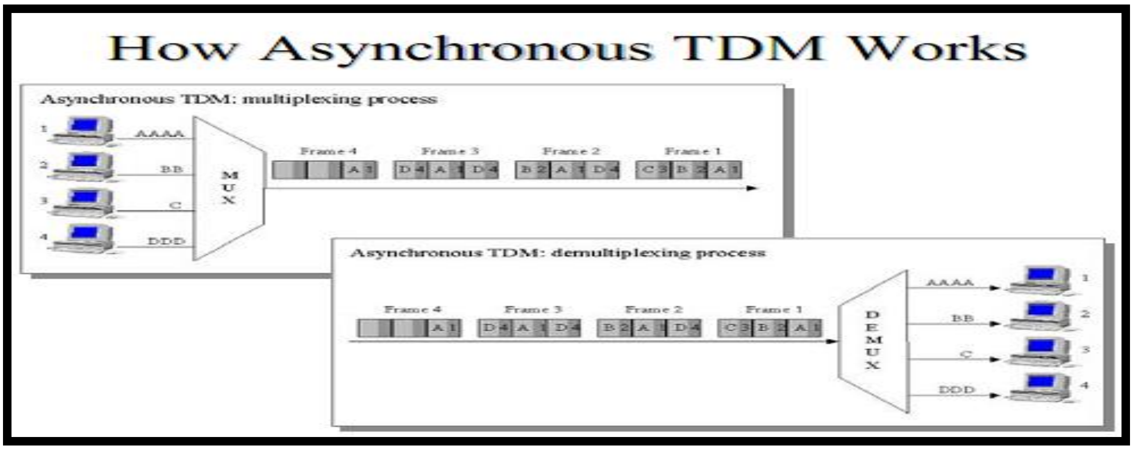


Asynchronous TDM

(or statistical time-division multiplexing)

- Each slot in a frame is **not** dedicated to the fix device
- The number of slots in a frame is not necessary to be equal to the number of input devices. More than one slots in a frame can be allocated for an input device.




How Asynchronous TDM Works
Asynchronous TDM: multiplexing process
AAAA
BB
C
DDD
MUX
Frame 4
Frame 3
Frame 2
Frame 1
Asynchronous TDM: demultiplexing process
DEMUX

❖ **Switching:-**

→ A network consists of many switching devices. In order to connect multiple devices, one solution could be to have a point to point connection in between pair of devices. But this increases the number of connection. The other solution could be to have a central device and connect every device to each other via the central device which is generally known as Star Topology. Both these methods are wasteful and impractical for very large network. The other topology also can not be used at this stage. Hence a better solution for this situation is SWITCHING. A switched network is made up of a series of interconnected nodes called switches.

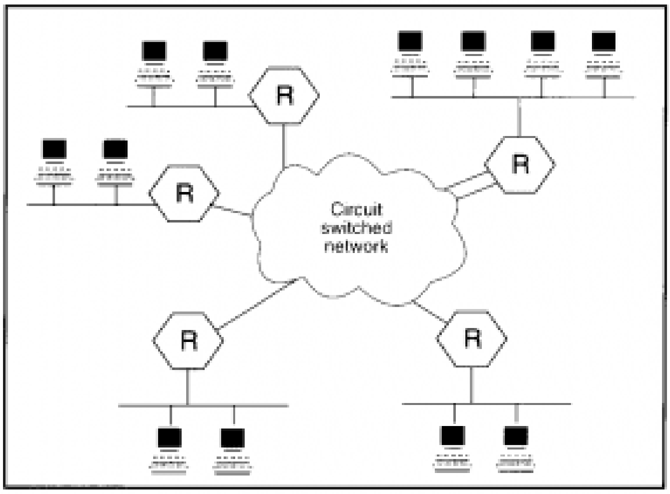
Types of Switching Techniques

→ There are basically three types of switching methods are made available. Out of three methods, circuit switching and packet switching are commonly used but the message switching has been opposed out in the general communication procedure but is still used in the networking application.

1) Circuit Switching
2) Packet Switching
3) Message Switching

Circuit Switching

→ Circuit Switching is generally used in the public networks. It come into existence for handling voice traffic in addition to digital data. How ever digital data handling by the use of circuit switching methods are proved to be inefficient. The network for Circuit Switching is shown in figure.



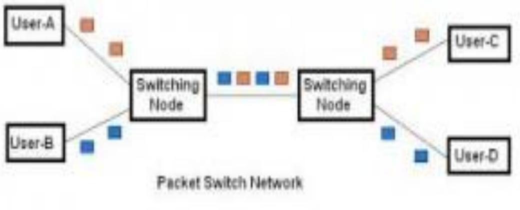
Circuit Switching Network

- Here the network connection allows the electrical current and the associated voice with it to flow in between the two respective users. The end to end communication was established during the duration of call.
- In circuit switching the routing decision is made when the path is set up across the given network. After the link has been sets in between the sender and the receiver then the information is forwarded continuously over the provided link.
- In Circuit Switching a dedicated link/path is established across the sender and the receiver which is maintained for the entire duration of conversation.

Packet Switching

→ In Packet Switching, messages are broken up into packets and each of which includes a header with source, destination and intermediate node address information. Individual Packets in packet switching technique take different routes to reach their respective destination. Independent routing of packets is done in this case for following reasons:

1. Bandwidth is reduces by the splitting of data onto different routes for a busy circuit.
2. For a certain link in the network, the link goes down during transmission the the remaining packet can be sent through the another route.



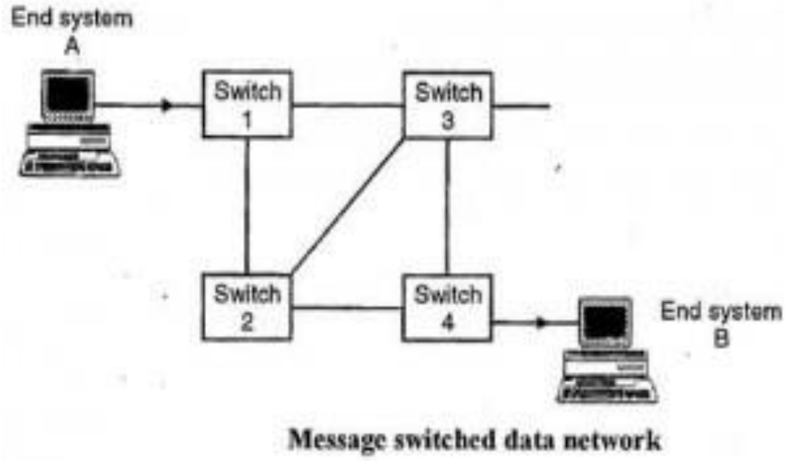
→ Packet Switching Network

- The major advantage of Packet switching is that they they are used for performing data rate conversion.
- When traversing the network switches, routers or the other network nodes then the packets are buffered in the queue, resulting in variable delay and throughput depending on the network’s capacity and the traffic load on network.
- Packet switching contrasts with another principal networking paradigm, circuit switching, a method which sets up a limited number of dedicated connections of constant bit rate and constant delay between nodes for exclusive use during the communication session.

- In cases where traffic fees are charged, for example in cellular communication, packet switching is characterized by a fee per unit of information transmitted.

Message Switching

→ In case of Message Switching it is not necessary to established a dedicated path in between any two communication devices. Here each message is treated as an independent unit and includes its own destination source address by its own. Each complete message is then transmitted from one device to another through internetwork.



Message Switching Data Network

- Each intermediate device receive the message and store it until the nest device is ready to receive it and then this message is forwarded to the next device. For this reason a message switching network is sometimes called as Store and Forward Switching.
- Message switches can be programmed with the information about the most efficient route as well as information regarding to the near switches that can be used for forwarding the present message to their required destination.
- The storing and Forwarding introduces the concept of delay. For this reasons this switching is not recommended for real time applications like voice and video.

Chapter 5: Networking Devices and Routing

❖ Layer 1 Devices :

❖ **NIC(NETWROK INTERFACE CARD) :**

- NIC Stands for Network Interface card. It is one of the most important computer network devices that are used for the data communication and to connect the computers with each other. It is plugged inside the computer either in the PCI slot or it is built-in the motherboard.
- A twisted pair UTP/STP with RJ45 connector is used to connect the computer with the Hub or Switch. Fiber optic cable can also be used to connect the computer with the hub or switch.
- A NIC can be wired or wireless and it has digital circuitry and microprocessor. A wireless NIC is used to connect the computers with each other wirelessly. There are different vendors of the NIC such as D-Link, 3Com, Intel, Realtek, Baylan and Baynet.
- Before buying and installing a network interface card in your computer make sure that it is compatible with the other network devices. NIC

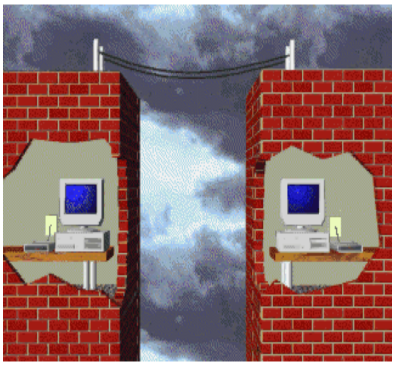
card operates on the Data Link and physical layer of the OSI layers model.

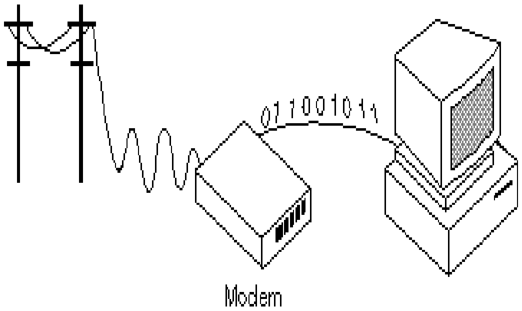
- For every computer in a network, it is required to have a NIC to communicate with other computers.
- Every NIC has unique MAC address and no two NIC cards from two different vendors can have the same MAC address. NIC has twisted pair, BNC and AUI sockets. The one end of the network cable is used to connect with the NIC and the other end is used to connect with the hub or switch.
  - NIC provides the fulltime connectivity for the data transmission.

NIC (NETWORK INTERFACE CARD)

- Sometimes computers do not communicate with each other due to the malfunctioning of the NIC.
- **The network interface cards problems can be resolved with the following tips.**
- Make sure that you have the updated and correct version of the LAN card's driver.
- Ensure that the LEDs of the NIC are working properly.
- Check that the network cable is properly connected at both ends.
- Right click on the network status icon on the right bottom of the desktop and click repair.
- Ensure that the TCP/IP settings are accurate.
- Disable the antivirus and firewall.
- If the problem still persists then try to replace the NIC with a new one.

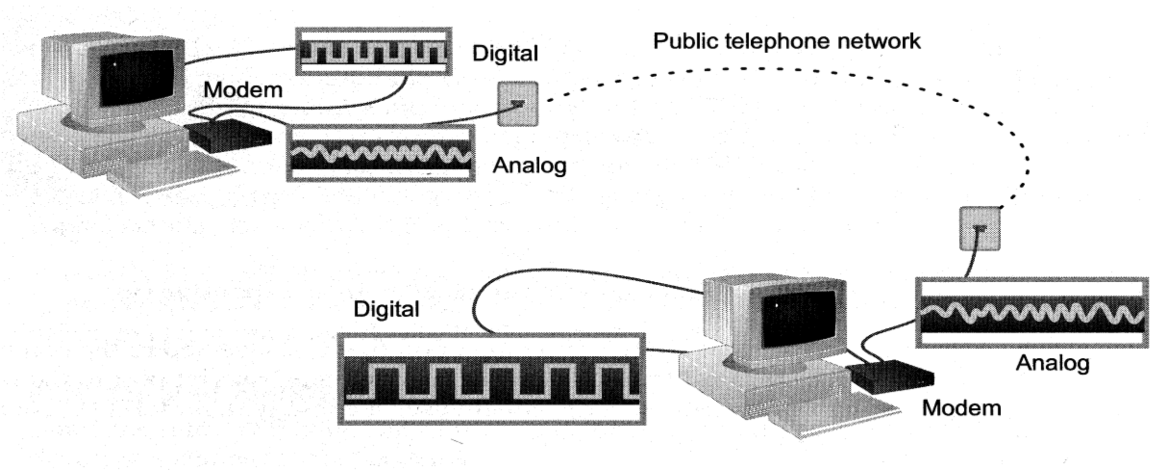
❖ **MODEM :**



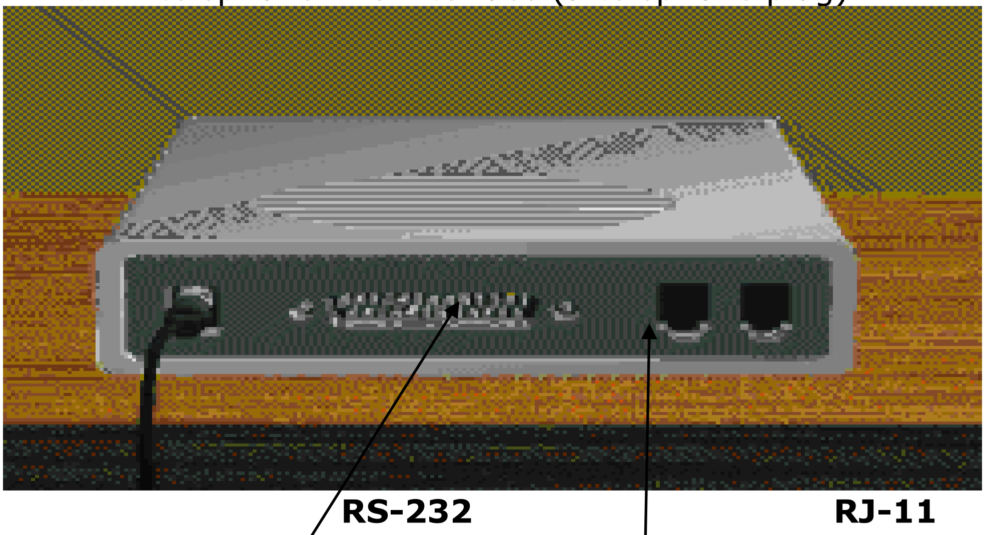


- Short for modulator-demodulator. A modem is a device or program that enables a computer to transmit data over, for example, telephone or cable lines.

- Computer information is stored digitally, whereas information transmitted over telephone lines is transmitted in the form of analog waves. A modem converts between these two forms.
- Allow computers to communicate over a telephone line
- Enable communication between networks or connecting to the world beyond the LAN
- Cannot send digital signal directly to telephone line
- **Sending end**: Modulate the computer's digital signal into analog signal and transmits
- **Receiving end**: Demodulate the analog signal back into digital form



- **Modems typically have the following I/O interface:**
- A serial RS-232 communication interface
- An RJ-11 telephone-line interface (a telephone plug)

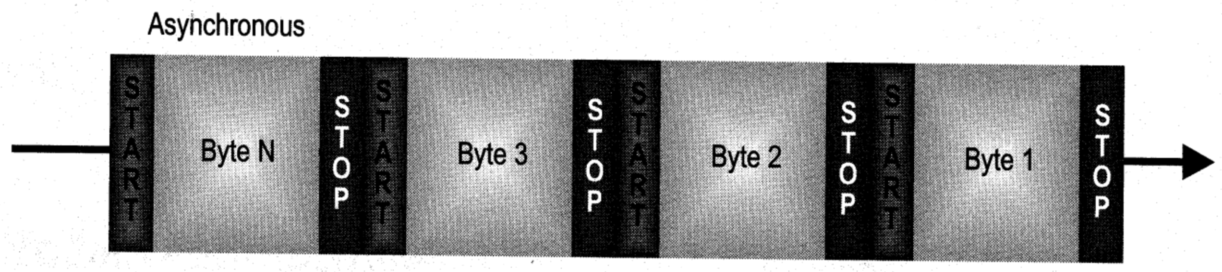


- **Modem Performance Measures :**
- **Baud rate -** the number of symbol change per second on the transmission line**.**
- **Bit per second (bps) -** number of bits transmitted per second.

❖ **Types of Modem :**

- Modems are classified according to the transmission method they use for sending and receiving data.
- **The two basic types of modems are as follows:**
- Asynchronous modems
- Synchronous modems

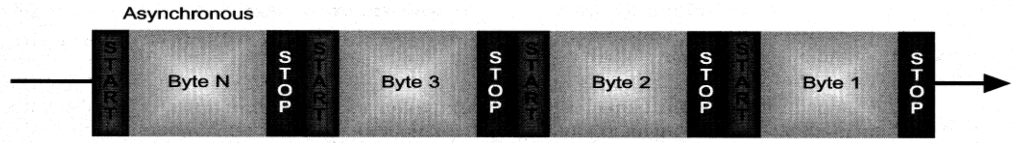
- **Asynchronous Modems :**
  - No clocking devices
  - Commonly used in telephone networks
  - Data is transmitted in a serial stream. Each character is turned into a string of 8 bits
  - Each of these characters is separated by one start bit and one or two stop bits

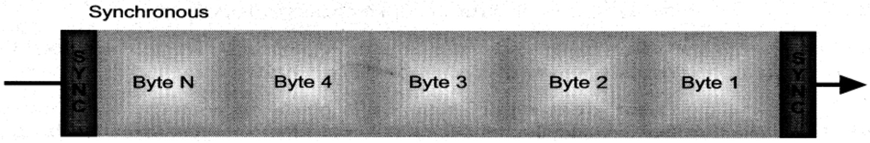


- Asynchronous transmission does not use a clocking mechanism to keep the sending and receiving devices synchronized.
- Instead, this type of transmission uses bit synchronization to synchronize the devices for each frame that is transmitted.
- In bit synchronization, each frame begins with a start bit that enables the receiving device to adjust to the timing of the transmitted signal.
- Asynchronous transmission is most frequently used to transmit character data and is ideally suited to environments in which characters are transmitted at irregular intervals, such as when users enter character data.
- Asynchronous transmission generally requires less expensive hardware than synchronous transmission.

- **Synchronous Modems :**
  - Need clocking devices
  - Data are transmitted in blocks
  - Used in digital networks
  - Synchronous transmission eliminates the need for start and stop bits by synchronizing the clocks on the transmitting and receiving devices.

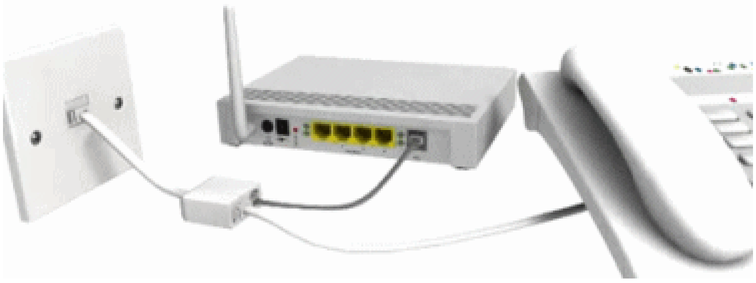
- **Synchronous transmission offers many advantages over asynchronous transmission**.
  - The overhead bits (synch, CRC, and end) comprise a smaller portion of the overall data frame, which provides for more efficient use of available bandwidth.
  - Synchronization improves error detection and enables the devices to operate at higher speeds.
- **The disadvantage of synchronous transmission is that**
  - The more complex circuitry necessary for synchronous communication is more expensive.
  - Network adapter cards commonly employ synchronous transmission methods.





- **Comparison : Asynchronous modems Vs Synchronous modems**
- **Asynchronous modems** are relatively simple and economic
  - Large overhead - can be up to 20 to 27% of the data traffic
  - Error control is done by using parity bit or higher layer protocols,
- **Synchronous modems** are relatively complicated and expensive
  - Seldom use in home market
  - Less overhead means higher efficiency
  - More sophisticated error control protocol is required.

❖ **DSL AND ADSL**:-

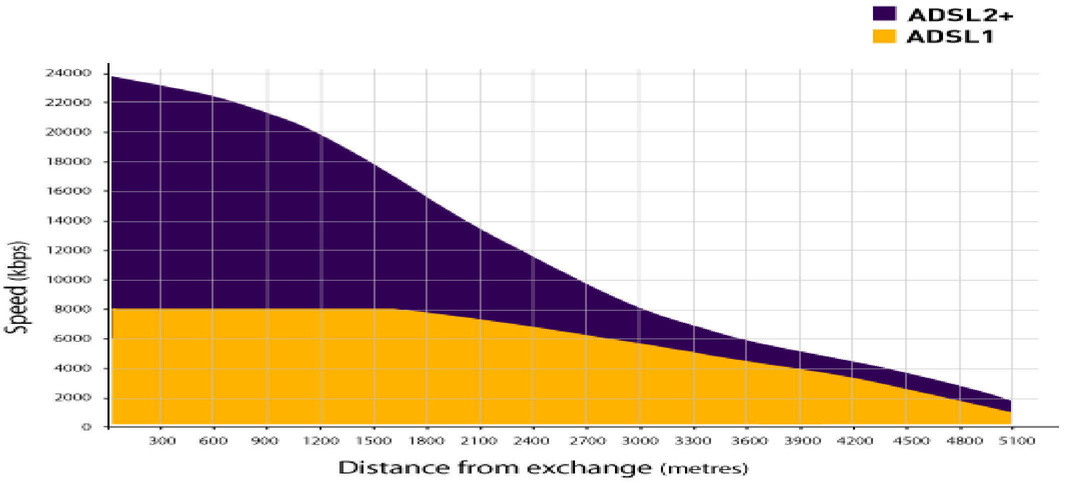


→

→ DSL (Digital Subscriber Line) is a common technology for bringing high-bandwidth (broadband) information to homes and small businesses over standard (copper) telephone lines. DSL comes in many different flavors, such as SDSL and ADSL2. The most common forms of DSL in the UK, ADSL (Asymmetric DSL) and ADSL2+, splits a single telephone line into separate voice and data channels, allowing you to make a phone call while surfing the Internet at the same time.

→ ADSL offers speeds of up to 8Mbps (Megabits per second) downstream and 448Kbps upstream (832Kbps on business lines). The technology is cheap, fast and easy to install (doesn't require an engineer) and reasonably reliable, although performance can suffer due to ISP congestion, distance from the local exchange (shorter lines are faster but anything over 6.5km is usually slow), poor home wiring and interference from other electrical devices. Each connection is fixed to a specific telephone line.

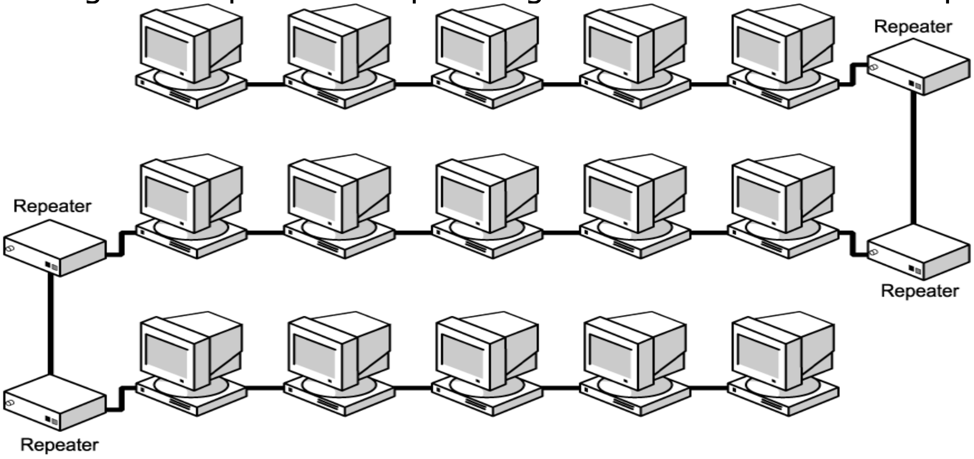
→ The latest ADSL2+ (ITU G.992.5) technology is capable of pushing download speeds at up to 24Mbps and uploads at up to 1.4Mbps, it also supports port bonding (linking several lines together for faster speeds) and has an improved range over ADSL. Both ADSL and ADSL2+ are "best efforts" broadband services, which means that bandwidth is shared between many users and can be highly variable - especially over long distances and at off-peak times (i.e. busy afternoons will slow the performance). The following graph shows what impact distance can have on speeds.



→ Users of these services should learn to understand common router statistics, which can help in diagnosing line problems. Figures for the following items will change depending on your line condition (e.g. expect them to be worse during thunderstorms that will cause extra interference):

❖ **Repeaters :**

- The purpose of a repeater is to extend the maximum range for the network cabling.
- A repeater is a network device that repeats a signal from one port onto the other ports to which it is connected (see Figure).
- Repeaters operate at the OSI Physical layer.
- 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.
- The advantages of repeaters are that they are inexpensive and simple.
- Some repeaters simply amplify signals. Although this increases the strength of the data signal, it also amplifies any noise on the network. In addition, if the original signal has been distorted in any way, an amplifying repeater cannot clean up the distortion.
- Multi-port repeaters are often called hubs.
- Hubs are very common internetworking devices. Generally speaking, the term hub is used instead of repeater when referring to the device that serves as the center of a star topology network.
- **Disadvantages :**
- it can't filter network traffic. Data, sometimes referred to as bits, arriving at one port of a repeater gets sent out on all other ports

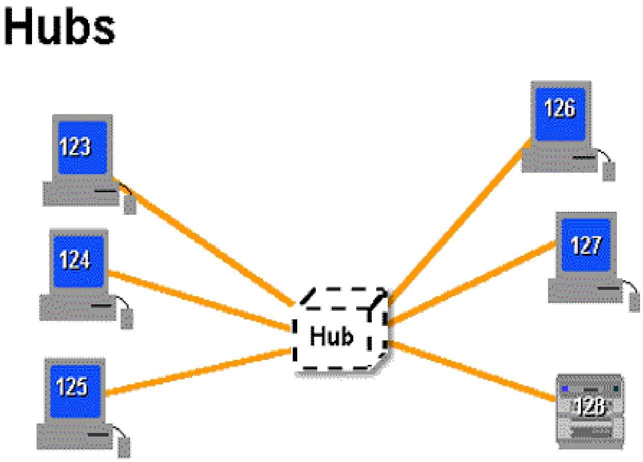


❖ Hub :

- Hubs, also called wiring concentrators, provide a central attachment point for network cabling.
- An unintelligent network device that sends one signal to all of the stations connected to it.
- Traditionally, hubs are used for star topology networks, but they are often used with other configurations to make it easy to add and remove computers without bringing down the network.
- Resides on Layer 1 of the OSI model

- **Hubs come in three types:**

- Passive
- Active
- Switching



- **Passive Hub:**

- Passive hubs do not contain any electronic components and do not process the data signal in any way.
- The only purpose of a passive hub is to combine the signals from several network cable segments.
- All devices attached to a passive hub receive all the packets that pass through the hub.
- Because the hub doesn't clean up or amplify the signals (in fact, the hub absorbs a small part of the signal),
- The distance between a computer and the hub can be no more than half the maximum permissible distance between two computers on the network. For example, if the network design limits the distance between two computers to 200 meters, the maximum distance between a computer and the hub is 100 meters.
- As you might guess, the limited functionality of passive hubs makes them inexpensive and easy to configure.

- That limited functionality, however, is also the biggest disadvantage of passive hubs.
- Often small networks use passive hubs, due to the fact that there are few machines on the LAN and small distances between them.

- **Active Hub:**
- Active hubs incorporate electronic components that can amplify and clean 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 cost considerably more than passive hubs.
- Because active hubs function in part as repeaters, they occasionally are called multiport repeaters.

- **Intelligent Hub :**
- Intelligent hubs are enhanced active hubs. Several functions can add intelligence 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. a switching hub acts like a very fast bridge.
- Switching hubs are the most expensive of hubs on the market. Often they are simply referred to as
  Switches. As for the exam, think of all types of hubs as simply a hub.

❖ Hub : Advantages And Disadvantages :

- **Advantages :**
- As an active hubs regenerate signals, it increases the distance that can be spanned by the LAN (up to 100 meters per segment).
- Hubs can also be connected locally to a maximum of two other hubs, thereby increasing the number of devices that can be attached to the LAN.
- Active hubs are usually used against attenuation, which is a decrease in the strength of the signal over distance.

- **Disadvantages :**
- Bandwidth is shared by all hosts i.e. 10Mbs shared by 25 ports/users.
- Can create bottlenecks when used with switches.
- Have no layer 3 switching capability.
- Active hubs are usually used against attenuation, which is a decrease in the strength of the signal over distance.

❖ Layer 2 Device :

❖ SWITCH:-

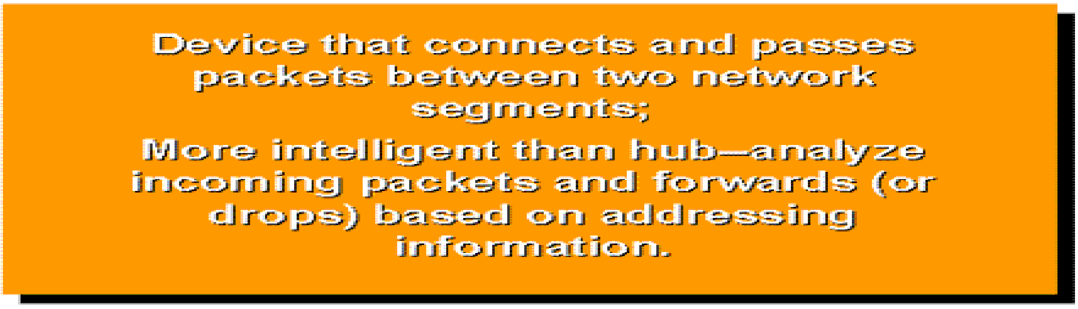
→ A **network switch** (also called **switching hub**, **bridging hub**, officially **MAC bridge** is a computer networking device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device. Unlike less advanced network hubs, a network switch forwards data only to one or multiple devices that need to receive it, rather than broadcasting the same data out of each of its ports.

→ A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model. Switches can also process data at the network layer (layer 3) by additionally incorporating routing functionality that most commonly uses IP addresses to perform packet forwarding; such switches are commonly known as layer-3 switches or multilayer switches. Beside most commonly used Ethernet switches, they exist for various types of networks, including Fibre Channel, Asynchronous Transfer Mode, and InfiniBand. The first Ethernet switch was introduced by Kalpana in 1990.

→ A switch is a device in a computer network that electrically and logically connects together other devices. Multiple data cables are plugged into a switch to enable communication between different networked devices. Switches manage the flow of data across a network by transmitting a received message only to the one or more devices for which the message was intended. Each networked device connected to a switch can be identified using a MAC address, allowing the switch to regulate the flow of traffic. This maximizes the security and efficiency of the network.

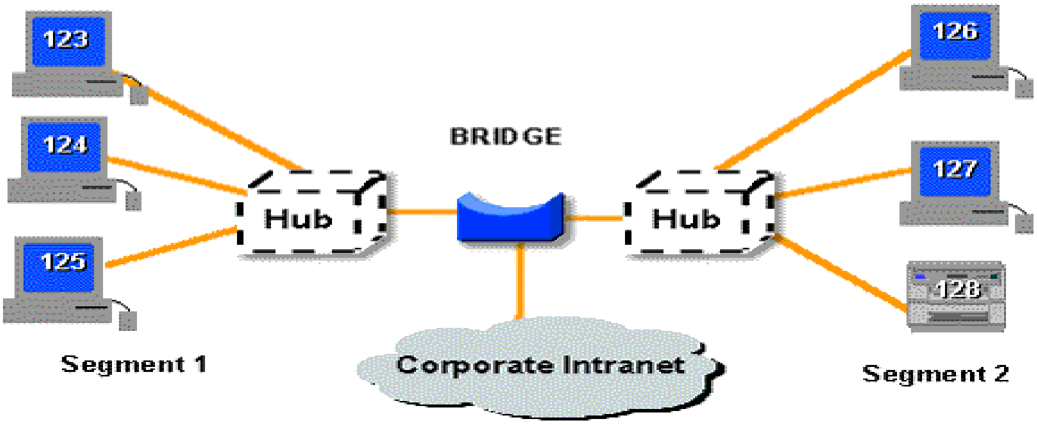
→ Essentially, when replacing a repeater hub with an Ethernet switch, the single large collision domain is split up into smaller ones, reducing the probability and scope of collisions and, as a result, increasing the potential throughput. Because broadcasts are still being forwarded to all connected devices, the newly formed network segment continues to be a broadcast domain.

❖ Bridge :

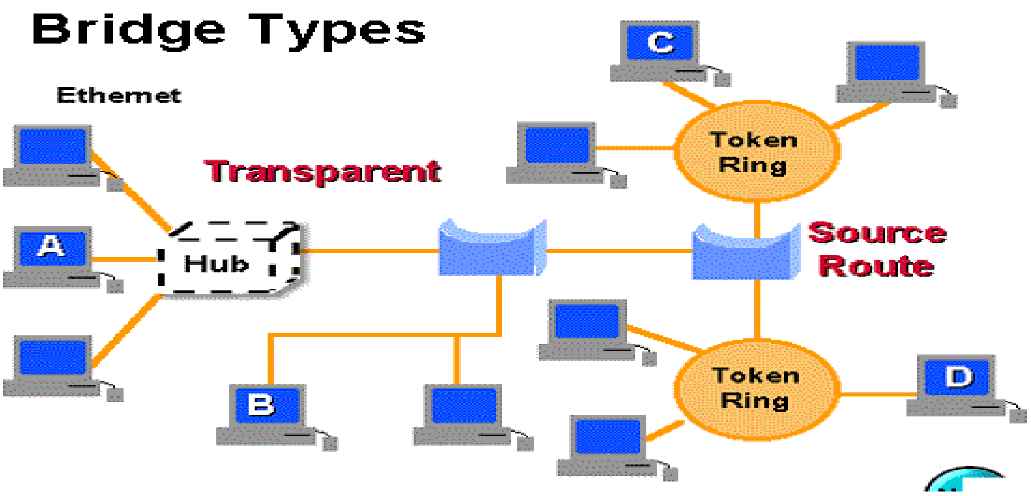


Device that connects and passes packets between two network segments;

More intelligent than hub—analyze incoming packets and forwards (or drops) based on addressing information.



- Bridges can extend the maximum size of a network.
- Bridge is a much more flexible device
- Bridges operate at the MAC sub layer of the OSI Data Link layer.
- Bridge is more selective and passes only those signals targeted for a computer on the other side.
- A bridge can make this determination because each device on the network is identified by a unique physical address.
- Bridges accomplish several things. First, they divide busy networks into smaller segments. If the network is designed so that most packets can be delivered without crossing a bridge, traffic on the individual network segments can be reduced.

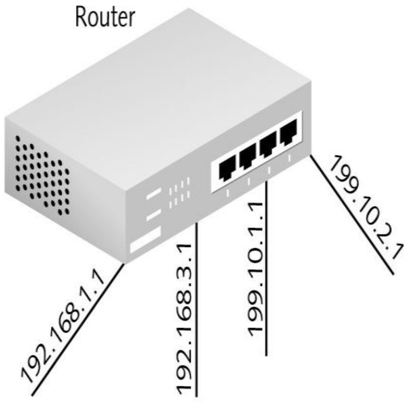


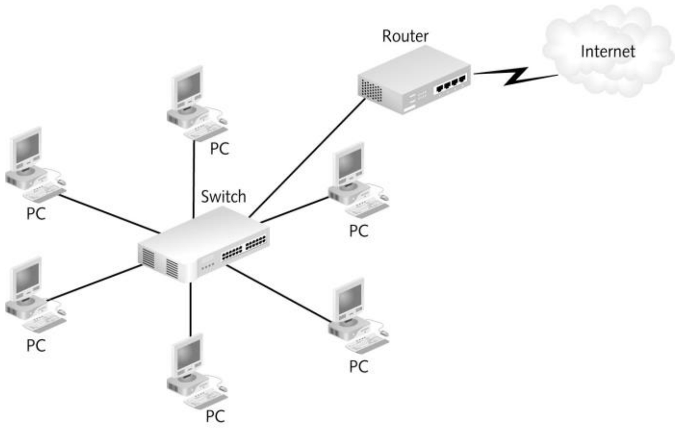
- **Source Route Bridge :**
  – Used in Token Ring networks.
  – The entire path (ring number and bridge number) is embedded within Packet
  • Search frame
  • Route discovery frame
- **Translational bridge :**
  – Used to convert one networking data format to another.
  • For example, from Token

❖ **Layer 3 Device :**

❖ **Router :**

- **Routing: The** process of determining systematically: How to forward messages toward the destination node based on its address.
- Routers are another type of internetworking device.
- These devices pass data packets between networks based on network protocol or layer 3 information.
- Routers have the ability to make intelligent decisions as to the best path for delivery of data on the network.
- Provide filtering and network traffic control
- Used on LANs and WANs
- Connect multiple segments and networks.
- Multiple routers create an "internetwork"
- Operate at the Network layer
- Create a table to determine how to forward packets
- Filtering and traffic control base on logical addresses.





- **Routers come in two general types:**
- **Static Routers**: These routers do not determine paths. Instead, you must configure the routing table, specifying potential routes for packets.
- **Dynamic Routers**: These routers have the capability to determine routes (and to find the optimum path among redundant routes) based on packet information and information obtained from other routers.
- Both static and dynamic routers use routing tables to pass packets on to remote sub networks.

❖ **Router : Advantages And Disadvantages :**

● **Advantages :**

- Can connect networks of different architecture
- Token Ring to Ethernet
- Choose best path through or to a network
- Create smaller collision domains
- Create smaller broadcast domains

● **Disadvantages :**

- Only work with routable protocols
- More expensive than hubs, bridges, and switches
- Routing table updates consume bandwidth.

❖ **Brouters :**

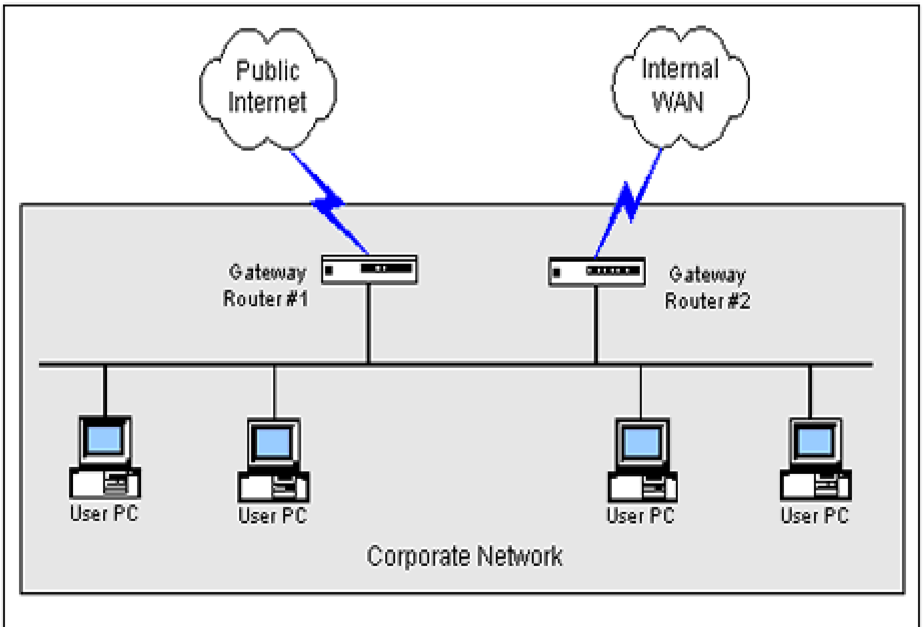
A brouter is a router that also can act as a bridge.

- A brouter attempts to deliver packets based on network protocol information, but if a particular Network layer protocol isn't supported, the brouter bridges the packet using device addresses.

- Hybrid device
- Functions as a router for routable protocols
- Functions as a bridge for non-routable protocols
- Operates at Data Link and Network layers.
- Operate at both the network layer for routable protocols and at the Data Link layer for non-routable protocols
- Handle both routable and non-routable features by acting as routers for routable protocols and bridges for non-routable protocols

❖ Gateway :

- A network gateway is an internetworking system capable of joining together two networks that use different base protocols.
- A network gateway can be implemented completely in software, completely in hardware, or as a combination of both. Depending on the types of protocols they support, network gateways can operate at any level of the OSI model.



Multiple Gateways

❖ WIRELESS NETWORK CONCEPTS:-

→ A wireless network device is a type of electronic that can be used on or used to help facilitate a wireless Internet network. There are many different devices that can fit within this definition, and the number only seems to be growing as wireless Internet becomes more and more widespread.

→ One of the most common examples is a router, which converts a fixed Internet signal into a wireless one and effectively creates a network that computers and other technology can connect to without the use of cables or other cords.

→ The things that are actually doing the connecting are also usually considered network devices, though, and this can include anything from computers and phones to e-readers and a wide range of "smart" gadgets. One of the core things that all have in common is the ability to both send and receive a wireless signal, and to connect instantaneously with other components on the same network.

❖ Basic Concept

→ In the world of Internet technology, wireless networks are becoming increasingly common. Not only are they growing in use in homes and offices, but they are also more and more commonplace in public areas like cafes, shopping malls, and restaurants.

→ The networks aren't usually worth much without devices that can jump onto them and use the signals provided for some other purpose.

→ Computers and many Internet-enabled phones use the signals primarily for browsing and e-mail capabilities. There are many more things that *can* be done, including storing and capturing data, routing cable television signals, and remotely controlling a range of things from garage door openers to light switches and home alarm systems.

❖ How They Work

→ This type of device works in cooperation with very specific wireless signals. The specifics tend to vary based on the engineering at issue as well as what it is the signal is being used to do, but in general, every device no matter its end purpose has both a sender and a receiver. The receiver picks up of the signal in the environment, and the sender converts it into something that can then be used for some other purpose within the network.

→ In order to take advantage of newer wireless signals and technologies, a wireless network device must usually be compatible with and up to date with that specific signal. Technology often changes more rapidly than product development. In many cases this requires upkeep and software installations on the user's part, and regular updating is usually very important.

❖ Router Capabilities and Signal Division

→ Wireless network devices can use a range of different signals. Much of this depends on the type of device and its purpose, as well as the sort of router anchoring the network as a whole. Wireless routers can operate on band signals such as 802.11a, 802.11b, 802.11g, and 802.11n. 802.11n requires a router with specific built-in technology. It offers a stronger signal and greater range compared to other wireless router networks.

→ Different bands and signals are also what allow these sorts of devices to run simultaneously without interfering with each other. Many households have wireless Internet as well as cable TV with a remote control and web-based data storage, both of which can be seen as basic wireless devices. Using the remote to flick to another channel on a TV does not interfere with using the Internet, any more than checking e-mail on a phone while also streaming video on a laptop would. This is because different devices typically use different bands and signals.

❖ Signal Conversions

→ Aside from being a device that broadcasts wireless signals, a network device may also be one that receives signals. Many video game consoles are examples of this sort of device when they're able to sync with a home's wireless router to allow online game play and other features.

→ Other examples of these devices include USB wireless adapters, wireless cards, some wireless keyboards and mice, and wireless printers. Any device or peripheral that operates by connecting to a wireless network is usually considered to be a wireless network device.

UNIT 3

Chapter 6 : Network Protocols

❖ Protocol & Packet :

Protocol:

A pre-defined rule for data transfer for example: IP, TCP, UDP, HTTP, FTP, SMTP

- The rules and encoding specifications for sending data. The protocol defines the format and meaning of the data that is exchanged. The protocols also determine whether the network uses a peer-to-peer or client/server architecture.
- **Protocol Roles:**
- Addressing and routing of messages
- Error detection
- Recovery
- Sequence and flow controls
- Example: HTTP protocol for communication between web browsers and servers.

Packet :

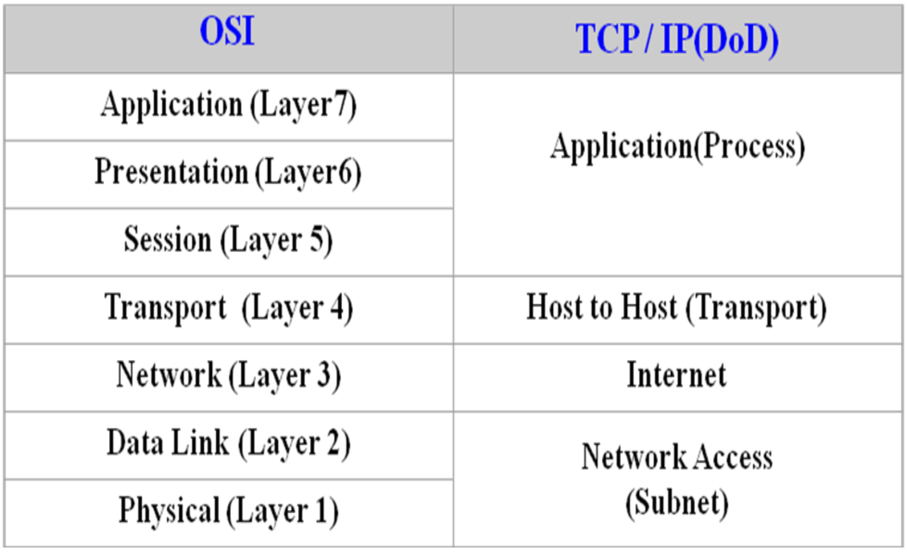
A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network.

- When any file (e-mail message, HTML file, Graphics Interchange Format file, Uniform Resource Locator request, and so forth) is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into "chunks" of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file (by the TCP layer at the receiving end).
- Packet" and "datagram" are similar in meaning. A protocol similar to TCP, the User Datagram Protocol (UDP) uses the term datagram.
- **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

❖ TCP/IP :

- A The TCP/IP protocol suite (also commonly called the Internet protocol suite) was originally developed by the United States Department of Defense (DoD) to provide robust service on large internetworks that incorporate a variety of computer types.
- Main purpose of this protocol was for it to be hardware-independent.
- In some literature, the TCP/IP protocol suite is referred to as the DoD model.
- In recent years, the Internet protocols constitute the most popular network protocols currently in use.

- One reason for the popularity of TCP/IP is that no one vendor owns it, unlike the IPX/SPX, DNA, SNA, or AppleTalk protocol suites, all of which are controlled by specific companies.
- TCP/IP evolved in response to input from a wide variety of industry sources.
- TCP/IP is the most open of the protocol suites and is supported by the widest variety of vendors. Virtually every brand of computing equipment now supports TCP/IP.
- This has lead to some problems, though. Because TCP/IP is an open standard, sometimes one vendor's implementation of TCP/IP does not work with another's implementation.



OSI	TCP/ IP(DoD)
Application (Layer7)	Application(Process)
Presentation (Layer6)	
Session (Layer 5)	
Transport (Layer 4)	Host to Host (Transport)
Network (Layer 3)	Internet
Data Link (Layer 2)	Network Access (Subnet)
Physical (Layer 1)	

- The model for the Internet protocol suite has four layers (refer to Figure). From this model, you can see

  The approximate relationships of the layers.

The DoD (TCP/IP) model's layers function as follows :

- **The Network Access layer** corresponds to the bottom two layers of the OSI model. This Correspondence enables the DoD protocols to coexist with existing Data Link and Physical layer standards.
- **The Internet layer** corresponds roughly to the OSI Network layer. Protocols at this layer move data between devices on networks.
- **The Host-to-Host layer** can be compared to the OSI Transport layer. Host-to-Host protocols enable peer communication between hosts on the internetwork. (At the time these protocols were designed, personal computers and workstations didn't exist, and all network computers were host computers. As a result, devices on TCP/IP networks are typically referred to as hosts. The concept of a client/server relationship didn't exist, and all communicating hosts were assumed to be peers.)
- **The Process/Application** layer embraces functions of the OSI Session, Presentation, and Application layers. Protocols at this layer provide network services.
- One huge advantage of using TCP/IP is that TCP/IP is required for communication over the Internet; thus the Internet can be used as a communication backbone.
- A large number of protocols are associated with TCP/IP. These different protocols are grouped into the following unofficial categories:

  General TCP/IP Transport Protocols
  TCP/IP Services

TCP/IP Routing

Advantages:

- Supports networking services better than the other Windows XP protocols
- Multiple routing protocols
- Good error detection and handling
- Works with most kinds of computers

Disadvantages:

- Not fast
- Not easy to use
- Requires
  - Fair degree of expertise
  - Careful planning
  - Constant maintenance and attention
- Mass of information and detail work.

❖ **FTP:-**

→ The **File Transfer Protocol** (**FTP**) is a standard network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet.

→ FTP is built on a client-server architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves using a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). SSH File Transfer Protocol (SFTP) is sometimes also used instead, but is technologically different.

→ The first FTP client applications were command-line applications developed before operating systems had graphical user interfaces, and are still shipped with most Windows, UNIX, and Linux operating systems. Many FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and FTP has been incorporated into productivity applications, such as Web page editors.

❖ **HTTP:-**

→ HTTP functions as a request-response protocol in the client-server computing model.

→ A web browser, for example, may be the *client* and an application running on a computer hosting a web site may be the *server*. The client submits an HTTP *request* message to the server. The server, which provides *resources* such as HTML files and other content, or performs other functions on behalf of the client, returns a *response* message to the client.

→ The response contains completion status information about the request and may also contain requested content in its message body.

→ A web browser is an example of a *user agent* (UA). Other types of user agent include the indexing software used by search providers (web crawlers), voice browsers, mobile apps, and other software that accesses, consumes, or displays web content.

❖ **SMTP:-**

→ **Simple Mail Transfer Protocol** (**SMTP**) is an Internet standard for electronic mail (email) transmission. First defined by RFC 821 in 1982, it was last updated in 2008 with the Extended SMTP additions by RFC 5321—which is the protocol in widespread use today.

→ SMTP by default uses TCP port 25. The protocol for mail submission is the same, but uses port 587. SMTP connections secured by SSL, known as

SMTPS, default to port 465 (nonstandard, but sometimes used for legacy reasons).

→ Although electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically use SMTP only for sending messages to a mail server for relaying. For receiving messages, client applications usually use either POP3 or IMAP.

→ Although proprietary systems (such as Microsoft Exchange and IBM Notes) and webmail systems (such as Outlook.com, Gmail and Yahoo! Mail) use their own non-standard protocols to access mail box accounts on their own mail servers, all use SMTP when sending or receiving email from outside their own systems.

❖ **POP3:-**

→ In computing, the **Post Office Protocol** (**POP**) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.

→ POP has been developed through several versions, with version 3 (**POP3**) being the last standard in common use before largely made obsolete by the more advanced IMAP.

→ POP supports simple download-and-delete requirements for access to remote mailboxes (termed mail drop in the POP RFC's).Although most POP clients have an option to leave mail on server after download, e-mail clients using POP generally connect, retrieve all messages, store them on the user's PC as new messages, delete them from the server, and then disconnect. Other protocols, notably IMAP, (Internet Message Access Protocol) provide more complete and complex remote access to typical mailbox operations.

→ In the late 1990s and early 2000s, fewer Internet Service Providers (ISPs) supported IMAP due to the storage space that was required on the ISP's hardware. Contemporary e-mail clients supported POP, then over time popular mail client software added IMAP support.

→ A POP3 server listens on well-known port 110. Encrypted communication for POP3 is either requested after protocol initiation, using the STLS command, if supported, or by POP3S, which connects to the server using Transport Layer Security (TLS) or Secure Sockets Layer (SSL) on well-known TCP port 995.

→ Available messages to the client are fixed when a POP session opens the maildrop, and are identified by message-number local to that session or, optionally, by a unique identifier assigned to the message by the POP server. This unique identifier is permanent and unique to the maildrop and allows a client to access the same message in different POP sessions. Mail is retrieved and marked for deletion by message-number. When the client exits the session, the mail mark.

❖ **SNMP:-**

→ **Simple Network Management Protocol** (**SNMP**) is an "Internet-standard protocol for managing devices on IP networks". Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more.[1] SNMP is widely used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

→ SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by Managing applications.

❖ **TELNET:-**

→ **Telnet** is an application layer protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

→ Telnet was developed in 1969 beginning with RFC 15, extended in RFC 854, and standardized as Internet Engineering Task Force (IETF) Internet Standard STD 8, one of the first Internet standards.

→ Historically, Telnet provided access to a command-line interface (usually, of an operating system) on a remote host. Most network equipment and operating systems with a configuration (including systems based on Windows NT). However, because of serious security concerns when using Telnet over an open network such as the Internet, its use for this purpose has waned significantly in favor of SSH.

→ The term *telnet* is also used to refer to the software that implements the client part of the protocol. Telnet client applications are available for virtually all computer platforms. *Telnet* is also used as a verb. *To telnet* means to establish a connection with the Telnet protocol, either with command line client or with a programmatic interface. For example, a common directive might be: "*To change your password, telnet to the server, log in and run the passed command.*" Most often, a user will be *telnetting* to a Unix-like server system or a network device (such as a router) and obtaining a login prompt to a command line text interface or a character-based full-screen manager.

❖ **ARP:-**

→ The **Address Resolution Protocol** (**ARP**) is a telecommunication protocol used for resolution of network layer addresses into link layer addresses, a critical function in multiple-access networks. ARP was defined by RFC 826 in 1982.It is Internet Standard STD 37. It is also the name of the program for manipulating these addresses in most operating systems.

→ ARP is used for mapping a network address to a physical address like an Ethernet address . ARP has been implemented with many combinations of network and data link layer technologies, like IPv4, Chaosnet, DECnet and Xerox PARC Universal Packet (PUP) using IEEE 802 standards, FDDI, X.25, Frame Relay and Asynchronous Transfer Mode (ATM). IPv4 over IEEE 802.3 and IEEE 802.11 is the most common case.

→ In Internet Protocol Version 6 (IPv6) networks, the functionality of ARP is provided by the Neighbor Discovery Protocol (NDP).

❖ **RARP:-**

→ The **Reverse Address Resolution Protocol** (**RARP**) is an obsolete computer networking protocol used by a client computer to request its Internet Protocol (IPv4) address from a computer network, when all it has available is its Link Layer or hardware address, such as a MAC address. The client broadcasts the request, and does not need prior knowledge of the network topology or the identities of servers capable of fulfilling its request.

- → RARP is described in Internet Engineering Task Force (IETF) publication RFC 903.It has been rendered obsolete by the Bootstrap Protocol (BOOTP) and the modern Dynamic Host Configuration Protocol (DHCP), which both support a much greater feature set than RARP.
- → RARP requires one or more server hosts to maintain a database of mappings of Link Layer addresses to their respective protocol addresses. Media Access Control (MAC) addresses needed to be individually configured on the servers by an administrator. RARP was limited to serving only IP addresses.
- → Reverse ARP differs from the Inverse Address Resolution Protocol (InARP) described in RFC 2390, which is designed to obtain the IP address associated with a local Frame Relay data link connection identifier. InARP is not used in Ethernet.

❖ IPX/SPX:

- The NetWare protocols have been designed with a high degree of modularity.
- This modularity makes the NetWare protocols adaptable to different hardware and simplifies the task of incorporating other protocols into the suite.
- Windows NT doesn’t use the IPX/SPX suite to communicate with NetWare resources.
- Microsoft instead developed a clone of IPX/SPX called NWLink—IPX/SPX Compatible Transport.
- IPX/SPX is generally smaller and faster than TCP/IP and, like TCP/IP, it is routable.
- However, it operates down to the Data Link layer of the OSI model so it is more dependent upon hardware devices than the TCP/IP protocol.
- IPX/SPX makes up the protocol suite that is used to transfer information on networks running the Novell NetWare operating system.
- **Internetwork Packet Exchange (IPX)** -Transfer information between devices.
  - Internetwork Packet Exchange
  - Connectionless protocol
  - Resides at the Network Layer
  - Responsible for network addressing and routing
- **Sequenced Packet Exchange (SPX)** - An extension of the IPX protocol.
  - Sequenced Packet Exchange
  - Connection-Oriented protocol
  - Resides at the Transport Layer
  - Uses services provided by IPX
  - Ensures reliable data delivery and manages sessions

● IPX/SPX Advantages/Disadvantages:

- Used mostly with Novell NetWare networks
- Common and outperforms TCP/IP
- Not supported on the Internet
- Typically found in private networks

❖ Apple Talk :

- AppleTalk is the computing architecture developed by Apple Computer for the Macintosh family of personal computers.
- Although AppleTalk originally supported only Apple's proprietary Local Talk cabling system, the suite has been expanded to incorporate both ethernet and token-ring Physical layers.
- Within Microsoft operating systems, AppleTalk is only supported by Windows NT Server. Windows NT Workstation and Windows 95 do not support AppleTalk.
- AppleTalk cannot be used for Microsoft-to-Microsoft operating system communication. It can be used only through Windows NT servers supporting Apple clients.
- AppleTalk originally supported networks of limited scope. The AppleTalk Phase II specification issued in 1989, however, extended the scope of AppleTalk to enterprise networks.
- Used only in Apple networks
- Routable Protocol
- AppleTalk Phase II allows this protocol to work with others
- AppleTalk divides groups of computers into Zones instead of Domains

❖ Server Messaging Blocks (SMB) :

One of the most popular protocols for PCs lets you share files, disks, directories, printers, and (in some cases) even COM ports across a network: this protocol is called the SMB (Server Message Block) standard.

- An SMB client or server can communicate with just about any other similar program.

❖ NETBIOS NAMES :

- Implement a NetBIOS naming scheme for all computers on a given network.
- NetBIOS is an interface that provides NetBIOS-based applications with access to network resources.
- Every computer on a Windows NT network must have a unique name for it to be accessible through the NetBIOS interface. This unique name is called a computer name or a NetBIOS name.
- NetBIOS (Network Basic Input/output System) is an application interface that provides
  PC-based applications with uniform access to lower protocol layers. NetBIOS was once most closely associated with the NetBEUI protocol—NetBEUI, in fact, is an abbreviation for NetBIOS Extended User Interface.

Assigning NetBIOS Names

- On a NetBIOS network, every computer must have a unique name.
- The computer name must be 15 characters long or fewer.
- NetBIOS name can include alphanumeric characters and any of the following special characters:
- NetBIOS names are not case-sensitive.

❖ Logical Link Control and Adaptation Protocol(L2CAP):

- The Logical Link Control and Adaptation Layer Protocol (L2CAP) is layered over the Baseband Protocol and resides in the data link layer.
- 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 kilobytes in length.

hardware/software/protocol description(For Bluetooth)

L2CAP has many functions:

- Multiplexing to allow several higher layer links, possibly based on different protocols.
- Segmentation and reassembly to allow transfer of larger packets than lower layers support.
- Quality of Service (QoS) management for higher layer protocols
- Optional error control and retransmissions.
- All applications must use L2CAP to send data. It is also used by Bluetooth's higher layers such as RFCOMM
- L2CAP provides the facilities needed by higher layer protocols to communicate across a Bluetooth link:

❖ RFCOMM :

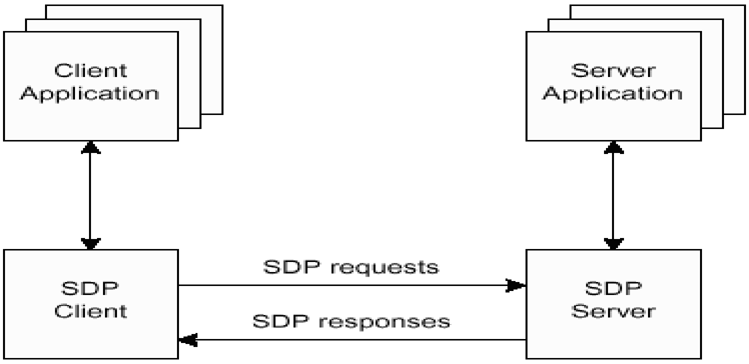
- RFCOMM is a simple transport protocol, which provides emulation of RS232 serial ports over the L2CAP protocol.
- The protocol is based on the ETSI (**European Telecommunications Standards Institute)** standard TS 07.10. a standard in the Telecom industry.
- The RFCOMM protocol supports up to 60 simultaneous connections between two BT devices. The number of connections that can be used simultaneously in a BT device is implementation-specific.

RFCOMM is commonly used:

- For Bluetooth GPS Receivers.
- To provide Bluetooth to legacy devices which used RS232 before. E.g., laser BarCode scanners, early mobile/foldable Bluetooth keyboards, wireless interface for hobby embedded system and robotic projects.
- As a basis for other legacy protocols like OBEX and PPP.

❖ Service Discovery Protocol (SDP) :

- The service discovery protocol (SDP) provides a means for applications to discover which services are available and to determine the characteristics of those available services.
- A specific Service Discovery protocol is needed in the Bluetooth environment, as the set of services that are available changes dynamically based on the RF proximity of devices in motion, qualitatively different from service discovery in traditional network-based environments.
- The service discovery protocol defined in the Bluetooth specification is intended to address the unique characteristics of the Bluetooth environment.
- SDP is a simple protocol with minimal requirements on the underlying transport.
- It can function over a reliable packet transport
- SDP uses a request/response model where each transaction consists of one request protocol data unit (PDU) and one response PDU



❖ Common Address Redundancy Protocol (CARP):

- The Common Address Redundancy Protocol, or CARP allows multiple hosts to share the same IP address.
- CARP is a free alternative to the Virtual Router Redundancy Protocol (VRRP).
- Its primary purpose is to allow multiple hosts on the same network segment to share an IP address. CARP works by allowing a group of hosts on the same network segment to share an IP address.
- This group of hosts is referred to as a redundancy group. The redundancy group is assigned an IP address that is shared among the group members.
- Within the group, one host is designated the master and the rest as back-ups.
- The master host is the one that currently holds the shared IP.
- It responds to any traffic or ARP requests directed towards it. Each host may belong to more than one redundancy group at a time
- CARP is a multicast protocol. It groups several physical computers together under one or more virtual addresses. Of these, one system is the master and responds to all packets destined for the group, the other systems act as hot spares.
- No matter what the IP and MAC address of the local physical interface, packets sent to the CARP address are returned with the CARP information.

CH 7. NETWORK ROUTING

❖ Routing protocol :

- A routing protocol is a protocol that specifies how routers communicate with each other, disseminating information that enables them to select routes then any two nodes on a computer network, the choice of the route being done by routing algorithms.
- Each router has a priori knowledge only of networks attached to it directly.
- A routing protocol shares this information first among immediate neighbors, and then throughout the network.
- This way, routers gain knowledge of the topology of the network.
  There are many types of routing protocols; three major classes are in widespread use on IP networks:

- **Interior gateway routing** via **link-state routing protocols**, such as **OSPF** and **IS-IS**
- **Interior gateway routing** via **path vector or distance vector protocols**, such as **RIP**, **IGRP** and **EIGRP**
- **Exterior gateway routing**. **BGP** v4 is the routing protocol used by the public Internet.

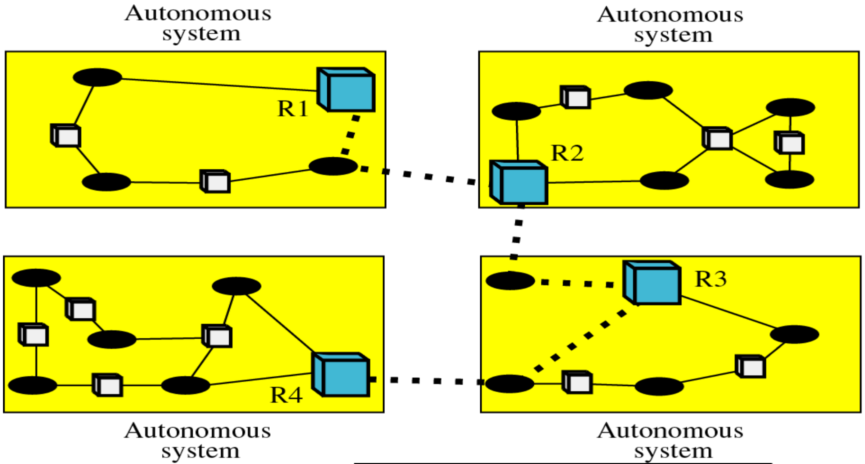
- **Link State Routing (Protocol):**

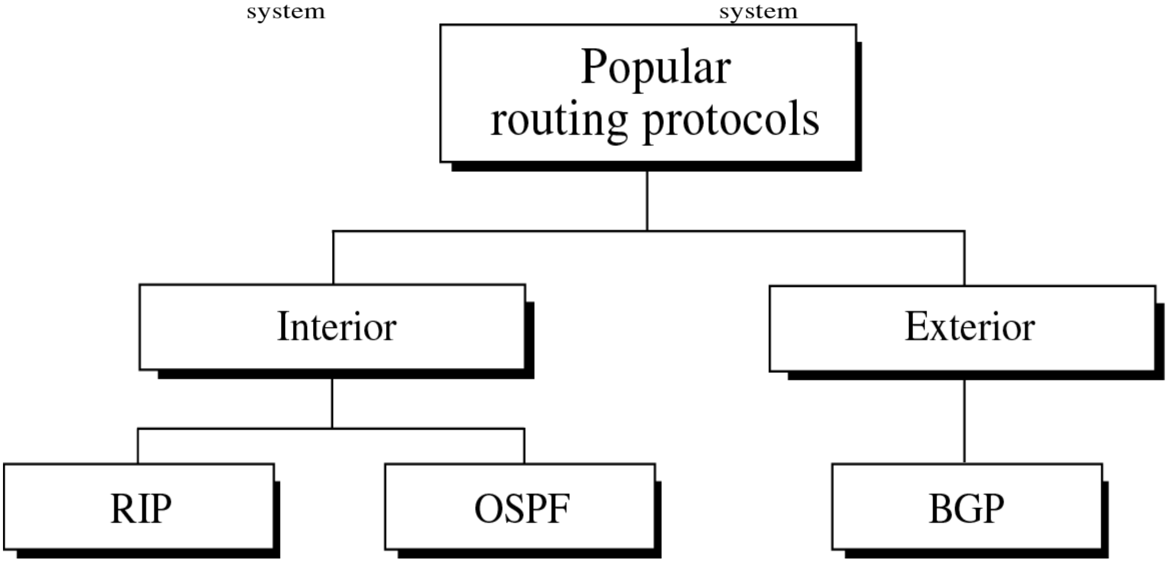
- The link-state protocol is performed by every switching node in the network (i.e. nodes that are prepared to forward packets; in the Internet, these are called routers).
- The basic concept of link-state routing is that every node constructs a map of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical path from it to every possible destination in the network. The collection of best paths will then form the node's routing table.

- **Distance Vector Routing (Protocol):**

- A distance-vector routing protocol requires that a router informs its neighbors of topology changes periodically and, in some cases, when a change is detected in the topology of a network.
- Compared to link-state protocols, which require a router to inform all the nodes in a network of topology changes, distance-vector routing protocols have less computational complexity and message overhead

- **Autonomous System (AS) :** Collection of networks with same policy
  - Single routing protocol. Usually under single administrative control.





❖ Interior Gateway Protocols (IGPs) :

- Interior Gateway Protocols (IGPs) exchange routing information within a single routing domain. A given autonomous system can contain multiple routing domains, or a set of routing domains can be coordinated without being an Internet-participating autonomous system.

Common examples include:

- **IGRP** (Interior Gateway Routing Protocol)
- **EIGRP** (Enhanced Interior Gateway Routing Protocol)
- **OSPF** (Open Shortest Path First)
- **RIP** (Routing Information Protocol)
- **IS-IS** (Intermediate System to Intermediate System)

■ **Interior Gateway Routing Protocol (IGRP) :**

- Interior Gateway Routing Protocol (IGRP) is a distance vector interior routing protocol (IGP) invented by Cisco.
- It is used by routers to exchange routing data within an autonomous system.
- IGRP was created in part to overcome the limitations of RIP (maximum hop count of only 15, and a single routing metric) when used within large networks.
- IGRP supports multiple metrics for each route, including bandwidth, delay, load, MTU, and reliability; to compare two routes these metrics are combined together into a single metric, using a formula which can be adjusted through the use of pre-set constants.
- The maximum hop count of IGRP-routed packets is 255 (default 100), and routing updates are broadcast every 90 seconds (by default).
- IGRP is considered a classful routing protocol. Because the protocol has no field for a subnet mask,.
- Classful protocols have become less popular as they are wasteful of IP address space.

■ **Enhanced Interior Gateway Routing Protocol (EIGRP) :**

- Enhanced Interior Gateway Routing Protocol - (EIGRP) is a Cisco proprietary routing protocol loosely based on their original IGRP. EIGRP is an advanced distance-vector routing protocol, with optimizations to minimize both the routing instability incurred after topology changes, as well as the use of bandwidth and processing power in the router.
- Widely used in many enterprise networks and in some ISP networks
- Multiprotocol (supports more than IP)
- Exhibits good scalability and rapid convergence
- Supports unequal cost load balancing.

■ **Open Shortest Path First** (**OSPF**) **:**

- Open Shortest Path First (OSPF) is a dynamic routing protocol for use in Internet Protocol (IP) networks.
- Specifically, it is a link-state routing protocol and falls into the group of interior gateway protocols, operating within a single autonomous system (AS).
- OSPF is perhaps the most widely-used interior gateway protocol (IGP) in large enterprise networks.
- It gathers link state information from available routers and constructs a topology map of the network.
- The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP diagrams.
- OSPF was designed to support variable-length subnet masking (VLSM) or Classless Inter-Domain Routing (CIDR) addressing models.

- OSPF detects changes in the topology, such as link failures, very quickly and converges on a new loop-free routing structure within seconds. It computes the shortest path tree for each route using a method based on Dijkstra's algorithm, a shortest path first algorithm.
- OSPF uses multicast addressing for route flooding on a broadcast network link.
- OSPF Version 2 for IPv4. The updates for IPv6 are specified as OSPF Version 3

■ Routing Information Protocol (RIP) :

- The Routing Information Protocol (RIP) is a dynamic routing protocol used in local and wide area networks.
- As such it is classified as an interior gateway protocol (IGP).
- It uses the distance-vector routing algorithm.
- It was first defined in RFC 1058 (1988).
- The protocol has since been extended several times, resulting in RIP Version 2 (RFC 2453).
- Both versions are still in use today, however, they are considered to have been made technically obsolete by more advanced techniques such as Open Shortest Path First (OSPF) and the OSI protocol IS-IS.
- RIP has also been adapted for use in IPv6 networks, a standard known as RIPng (RIP next generation), published in RFC 2080 (1997).
- There are three versions of the Routing Information Protocol: RIPv1, RIPv2, and RIPng.

■ Intermediate system to intermediate system (IS-IS) :

- Intermediate system to intermediate system (IS-IS), is a protocol used by network devices (routers) to determine the best way to forward diagrams through a packet-switched network, a process called routing.
- IS-IS is a link-state routing protocol, meaning that it operates by reliably flooding Link State information throughout a network of routers. Each router then independently builds a picture of the network's topology. Packets or datagrams are forwarded based on the best topological path through the network to the destination.
- The protocol was defined in ISO/IEC 10589:2002 as an international standard within the Open Systems Interconnection (OSI) reference design.
- IS-IS is not an Internet standard, however IETF republished the standard in RFC 1142 for the Internet community.

❖ Exterior Gateway Protocol (EGP):

- Exterior Gateway Protocol (EGP) is a now obsolete routing protocol for the Internet originally specified in 1982 by Eric C. Rosen of Bolt, Beranek and Newman, and David L. Mills.
- EGP is a simple reach ability protocol, and, unlike modern distance-vector and path-vector protocols, it is limited to tree-like topologies.
- examples include:
- **BGP** (Border Gateway Protocol).

■ Border Gateway Protocol (BGP):

- The Border Gateway Protocol (BGP) is the core routing protocol of the Internet.
- It maintains a table of IP networks or 'prefixes' which designate network reach ability among autonomous systems (AS).
- It is described as a path vector protocol.

- BGP does not use traditional Interior Gateway Protocol (IGP) metrics, but makes routing decisions based on path, network policies and/or rule sets.
- BGP was created to replace the Exterior Gateway Protocol (EGP) routing protocol to allow fully decentralized routing.
- This allowed the Internet to become a truly decentralized system.

Operation:

- BGP neighbors, or peers, are established by manual configuration between routers to create a TCP session on port 179.
- A BGP speaker will periodically send 19-byte keep-alive messages to maintain the connection (every 60 seconds by default). Among routing protocols,
- BGP is unique in using TCP as its transport protocol.
- When BGP is running inside an autonomous system (AS), it is referred to as Internal BGP (IBGP or Interior Border Gateway Protocol).
- When it runs between autonomous systems, it is called External BGP (EBGP or Exterior Border Gateway Protocol).
- Routers on the boundary of one AS, exchanging information with another AS, are called border or edge routers.
- In the Cisco operating system, IBGP routes have an administrative distance of 200, which is less preferred than either external BGP or any interior routing protocol.
- Other router implementations also prefer EBGP to IGPs, and IGPs to IBGP.
- BGP Can be used in two scenarios
  - Internally, inside an Autonomous System
    - Known as **IBGP** (Internal BGP)
  - Externally, between peers
    - Known as **EBGP** (External BGP)

❖ **Types of Routing**

→ There are three basic methods to build a routing table on any Networking Device.

1. **Static Routing**
2. **Dynamic Routing**
3. **Default Routing**

→ **Static Routing:**

→ A **static routing** occurs when you manually add routes in each Router's Routing table, Routing table should create, maintain, and update by a network administrator, manually.

→ A static route to every network must be configured on every router for full connectivity. This provides a granular level of control over routing, but quickly becomes impractical on large networks.

→ Routers will not share static routes with each other, thus reducing CPU/RAM overhead and saving bandwidth. However, static routing is not fault-tolerant, as any change to the routing infrastructure (such as a link going down, or a new network added) requires manual intervention.

→ Routers operating in a purely static environment cannot seamlessly choose a better Route if a link becomes unavailable. Static routes have an Administrative Distance (AD) of **1**, and thus are always preferred over dynamic routes, unless the default AD is changed. A **static route** with an **adjusted AD** is called a **floating static route.**

- The following briefly outlines the advantages and disadvantages of static routing:

→ **Advantages of Static Routing:**

1. Minimal CPU/Memory overhead
2. There is no bandwidth update between Routers, which means you will Save bandwidth on WAN links.
3. It adds security because the administrator can choose Routing access to certain networks only.

→ **Disadvantages of Static Routing:**

1. If any Infrastructure changes must be manually adjust the Configuration in complete network.
2. No "dynamic" fault tolerance if a link goes down
3. Administrator must understand the complete internetwork and how each Router connected to configure properly.
4. Impractical on large network

→ **Dynamic Routing:**

→ A Dynamic Routing is when protocols are used to find networks and update Routing tables on Routers.

→ A **dynamic** routing table is created, maintained, and updated by a routing protocol running on the router. Examples of routing protocols include **RIP** (Routing Information Protocol), **EIGRP** (Enhanced Interior Gateway Routing Protocol), and **OSPF** (Open Shortest Path First).

→ Routers do share dynamic routing information with each other, which increases CPU, RAM, and bandwidth usage. However, routing protocols are capable of dynamically choosing a different (or better) path when there is a change to the routing infrastructure.

❖ **Difference between Routing Protocols and Routed Protocols**

→ Do not confuse **routing protocols** with **routed protocols**:

→ A **routed protocol** is a Layer 3 protocol that applies logical addresses to devices and routes data between networks (such as IP)

→ A **routing protocol** dynamically builds the network, topology, and next hop information in routing tables (such as RIP, EIGRP, etc.)

→ The following briefly outlines the advantages and disadvantages of dynamic routing:

→ **Advantages of Dynamic Routing:**

1. Simpler to configure on larger networks
2. Will dynamically choose a different (or better) route if a link goes down
3. Ability to load balance between multiple links

→ **Disadvantages of Dynamic Routing:**

1. Updates are shared between routers, thus consuming bandwidth
2. Routing protocols put additional load on router CPU/RAM
3. The choice of the "best route" is in the hands of the routing protocol, and not the network administrator.

→ **Default Routing:**

→ A default routing is used only when one exit path from the Router. Default Routing can configure like a static route with the ip route command, but use 0.0.0.0 0.0.0.0 for the IP network and subnet mask followed by the next hop router's IP address or Exit interface of the local Router.

→ Have to also use the ip classless command since there aren't any routes in the routing table. ip classless is enabled by default in IOS version 12.

- **Command Syntax for Default Routing on Cisco Router**
- Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.2
  Router (config) #ip classless.

UNIT 4

Chapter 8 : IP Addressing

❖ IP Address:

- Unique logical address of any computer consider as a ip address.
- It has 2 types:-

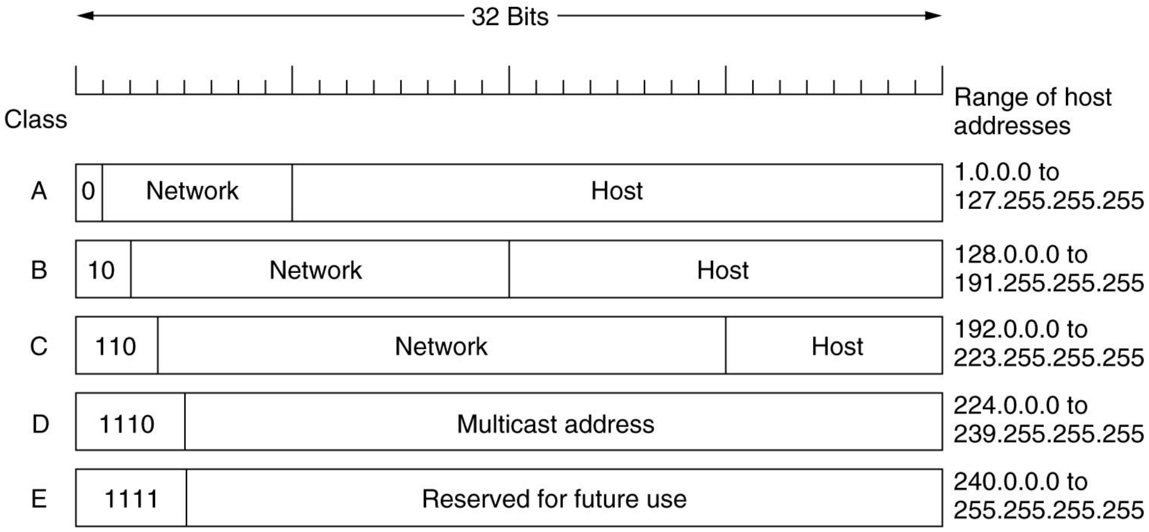
1) IPv4
2) IPv6

❖ IPv4 :-

- The IP address is a 32 bit address.
- Identifies the network and the host on a given network.
- Divided into two parts first part identifies the network, second part identifies the host on the network
- The format is not the same for each address.
- The 32 bit number is represented in the following format.
- xxx.xxx.xxx.xxx
- Where xxx is the decimal representation of the binary bit string.
- Example: 142.110.3.4

10001110 01101110 00000011 00000100

❖ Classes of IP Addresses :



32 Bits
Class
Range of host addresses
A
0
Network
Host
1.0.0.0 to 127.255.255.255
B
10
Network
Host
128.0.0.0 to 191.255.255.255
C
110
Network
Host
192.0.0.0 to 223.255.255.255
D
1110
Multicast address
224.0.0.0 to 239.255.255.255
E
1111
Reserved for future use
240.0.0.0 to 255.255.255.255

■ **Class A :**

- Used for small number of networks and large number of hosts.
- First byte (8 bits) represents the network address.
- Last 3 bytes (24 bits) represent the host address.
- Class A addresses have a first bit of 0.
- Class A network addresses range from 0 to 127.

■ **Class B :**

- Provide an equal number of networks and hosts.
- First two bytes are network address and last two bytes are host addresses.

- First two bits of a class B address are 10.
- Network addresses range from 128 to 191.

■ **Class C:**

- Greater number of network addresses fewer host addresses.
- First three bits are 110.
- Network addresses range form 192-223.

■ **Class D :**

- Used for special multicast addresses.
- First four bits 1110.

■ **Class E :**

- Used for experimental purposes
- first four bits 1111

❖ Subnets :

- Subnets are used to divide a large network into smaller networks.
- Each address allows for one network address and many hosts (ie all hosts are on the same network).
- Subnet masks are used to create many subnets within the same network address.

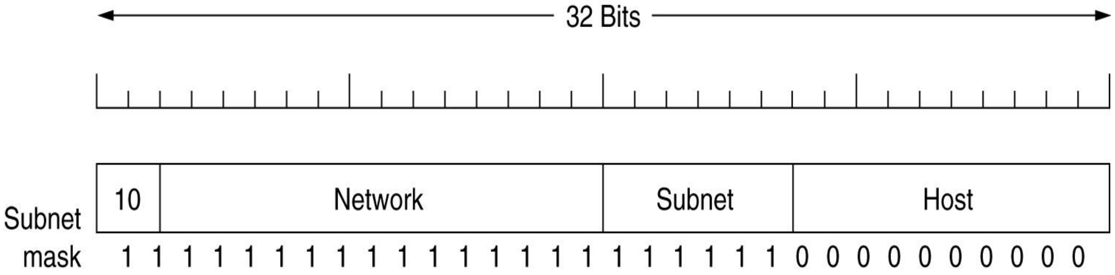
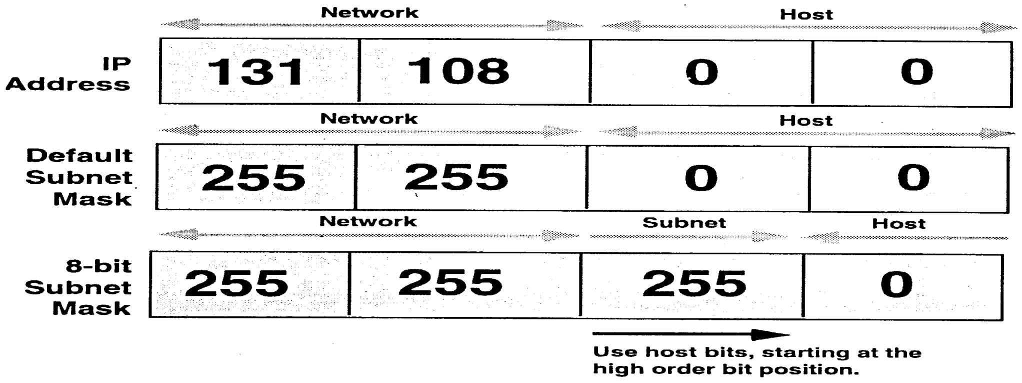


Fig: A class B network sub netted into 64 subnets

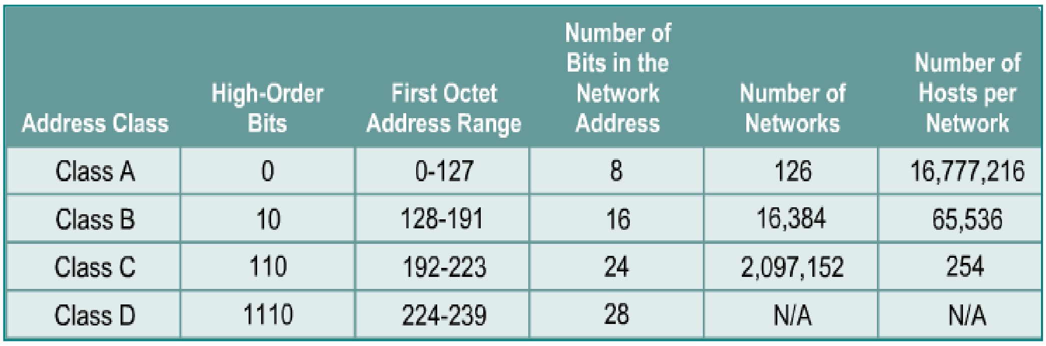
❖ Subnet masks :

- A bit string applied to an address.
- If the bit is on the corresponding bit in the address is considered to be a network bit.
- The network mask is known locally only.



- **Layout of the subnet mask**
  - **binary 1 for network bits**
  - **binary 1 for subnet bits**
  - **binary 0 for host bits**

Fig: Subnet Mask for Class B address



Address Class	High-Order Bits	First Octet Address Range	Number of Bits in the Network Address	Number of Networks	Number of Hosts per Network
Class A	0	0-127	8	126	16,777,216
Class B	10	128-191	16	16,384	65,536
Class C	110	192-223	24	2,097,152	254
Class D	1110	224-239	28	N/A	N/A

❖ Sub netting :

- A network is divided into several smaller networks with each sub network (or subnet) having its sub network address.

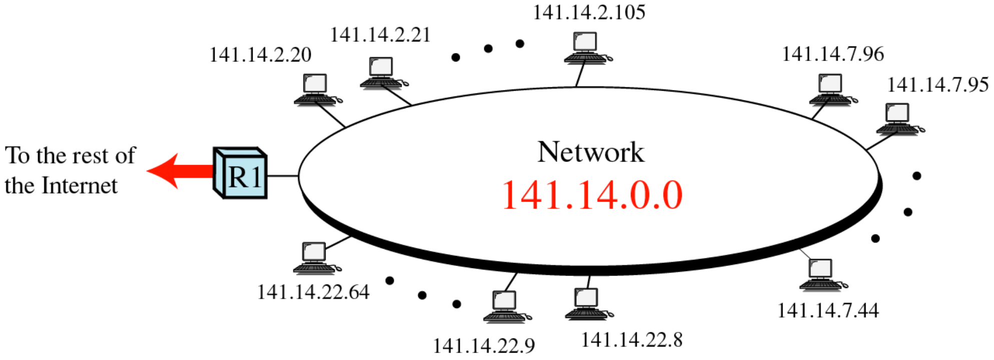


Fig: Not sub netted

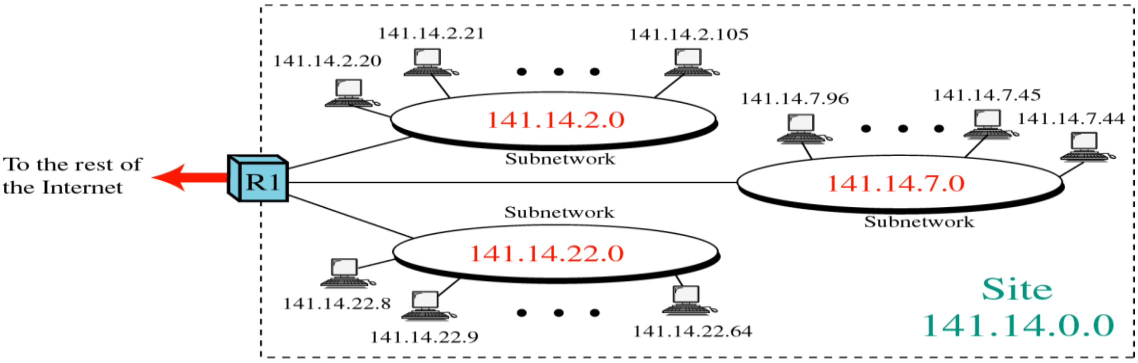
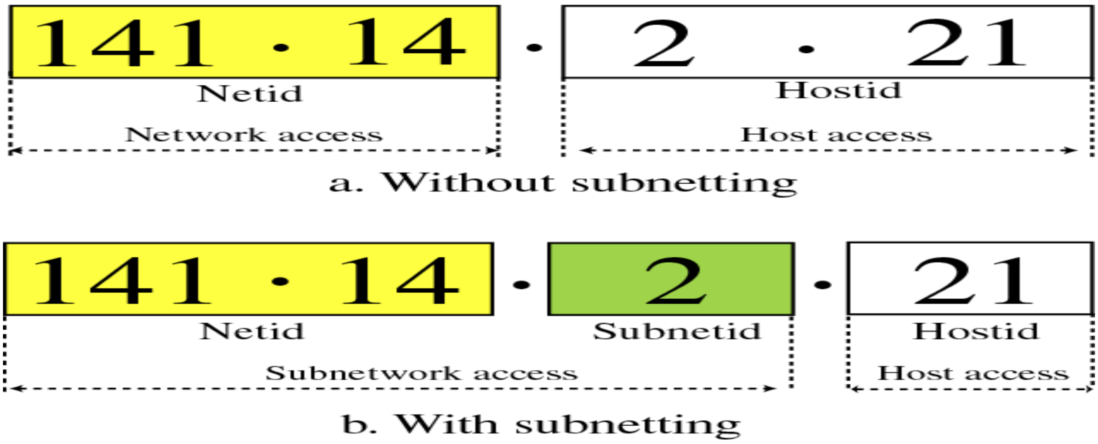


Fig: Sub netted



a. Without subnetting

b. With subnetting

Fig: Three levels of hierarchy : netid, subnetid, and hostid

❖ Super netting :

- Combining several class C addresses to create a larger range of addresses.

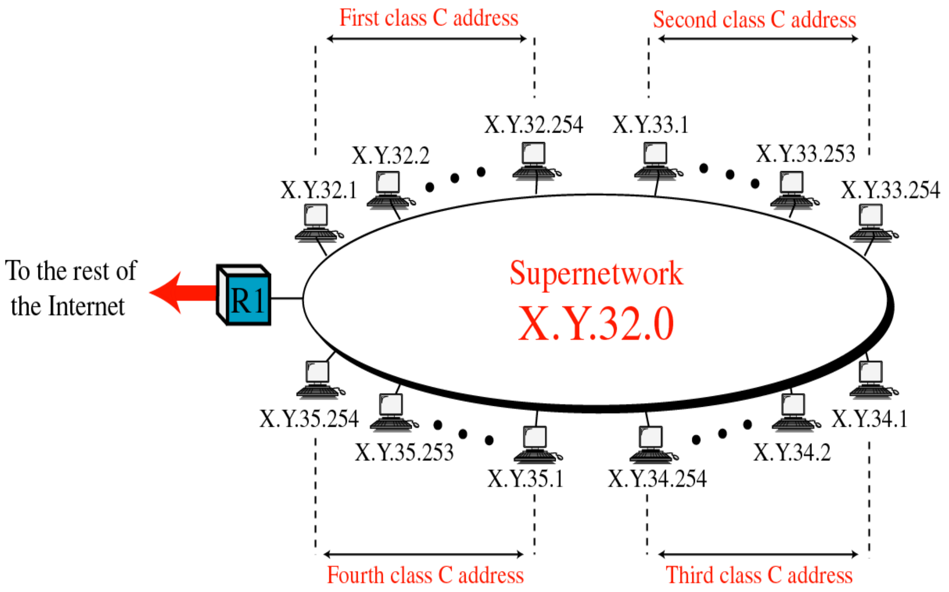
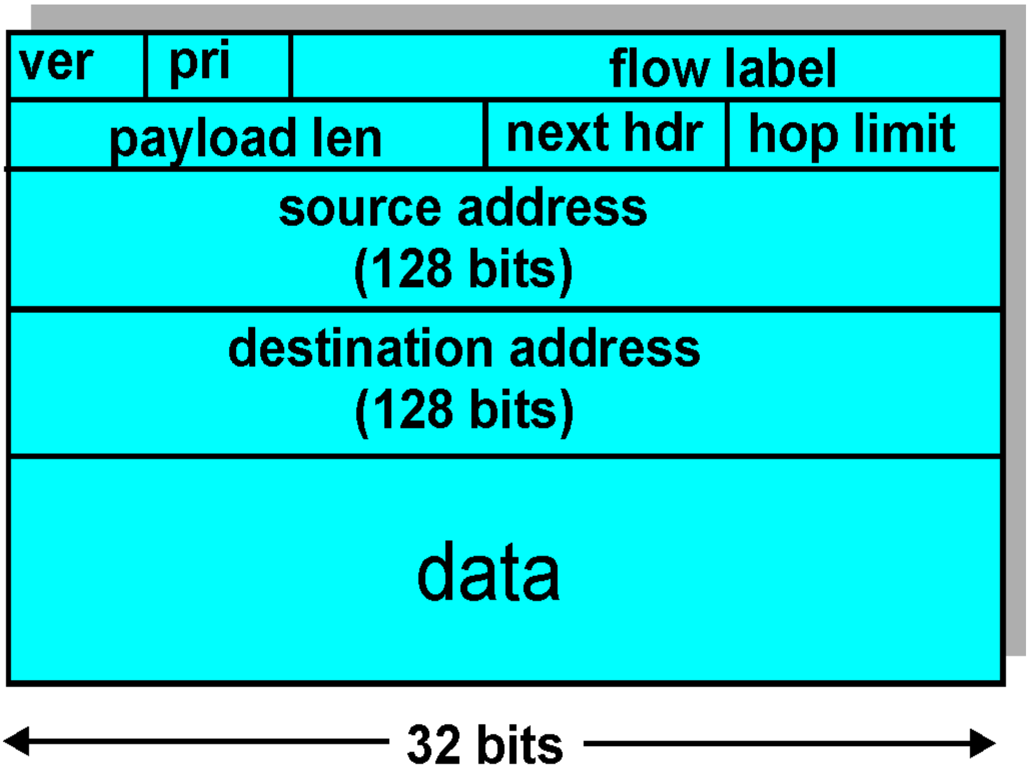


Fig: 4 class C addresses combine to make one super network

❖ IPV6 :

- IPv6 was designed to take an evolutionary step from IPv4.. Functions that work in IPv4 was kept in IPv6.Functions that didn't work were removed. The changes from IPv4 to IPv6 fall primarily into the following categories:
- ■ Header Format Simplification
- ■ Improved Support for Options
- ■ Expanded Routing and Addressing Capabilities
- ■ Quality-of-Service Capabilities
- ■ Authentication and Privacy Capabilities
- IPV6 is Datagram Protocol.
- Routing via RIP, OSPF, IS-IS, BGP
- End-to-end reliability via TCP
- Semantics are very similar to IPv4
- Larger addresses
- More emphasis on security
- IPv6 is a Network Protocol with many more addresses than IPv4:
- 340,282,366,920,938,463,374,607,431,768,211,456 available addresses.
- With so many addresses we can overcome the shortage in IPv4 supply and continuing support the growth of Internet.
- In IPv6 some tasks are simpler than in IPv4: (Auto-configuration, Renumbering, Multicast, IP Mobility, etc.)
- IPv6 Enables Innovation. Particularly for applications without NAT .
- IPv6 addresses are represented by Hexadecimal numbers.
- Example: 2001:DB8:12FF:1231:FFB5::F9DA/64.
- In IPv6 there is not Network Mask, only Prefix Length.
- In IPv6 the header is always 40 bytes long, extensions are listed as “next header”.
- In IPv6 there is no Broadcast, only Multicast.
- In IPv6 there is no ARP or IGMP, ICMPv6 takes those jobs.
- IPv6 has 128-bit (16-byte) source and destination IP addresses. Although 128 bits can express over 3.4□10^{38} possible combinations, the large address space of IPv6 has been designed to allow for multiple levels of subnetting and address allocation from the Internet backbone to the individual subnets within an organization.



- IPv6 header is simpler than IPv4
  - IPv4: 14 fields, variable length (20 bytes +)
  - IPv6: 8 fields, fixed length (40 bytes)
- Header fields eliminated in IPv6
  - Header Length
  - Identification
  - Flag
  - Fragmentation Offset
  - Checksum
- Header fields enhanced in IPv6
  - Traffic Class
  - Flow Label

Chapter 9: Windows Server 2003

❖ Installing and Configuring Windows Server 2003 :

As an experienced IT professional, you have no doubt spent considerable time installing Windows platforms.

Some of the important and enhanced considerations when installing Windows Server 2003 are :

- **Bootable CD-ROM installation :**
  Windows Server 2003 can be installed directly from the CD-ROM. There is no support for starting installation from floppy disks.

- **Improved graphical user interface (GUI) during setup :**
  Windows Server 2003 uses a GUI during setup that resembles that of Windows XP

- **Product activation :**

Retail and evaluation versions of Windows Server 2003 require that you activate the product.

Volume licensing programs, such as Open License, Select License, or Enterprise Agreement, do not require activation.

Following Step required installing Windows 2003.

1. Configure the computer's BIOS or the disk controller BIOS to boot from CD-ROM. If you are not sure how to configure your computer or disk controller to boot from CD-ROM, consult your hardware documentation.

2. Insert the Windows Server 2003 installation CD-ROM into the CD-ROM drive and restart the computer.

3. After configuring the system for booting from a CD, the Windows Setup screen appears.

At this point, Setup is loading the driver files it needs to continue with installation.

4. The "Time Limited" warning screen appears with the option of Continuing Setup or Quitting.

Press ENTER to Continue Setup or F3 to Quit and reboot the system.

5. The "Welcome to Setup" screen appears with the option of Continuing Setup, Repair a previous installation, or Quitting.

- Press ENTER to Continue Setup.
- You may also choose R to Repair or F3 to Quit and reboot the system.

6. The "Windows Licensing Agreement" screen, otherwise known as "EULA," displays the legal in's and out's of this particular software package.

- You may press F8 to signify that you agree with the terms, hit ESC if you do not agree and PAGE UP or PAGE DOWN to scroll through each screen. Note: If you do not agree to the terms, setup will quit and reboot the system.

7. Hard drive partition information is now displayed. This varies with each systems hardware configuration.

8. Continue to create partitions until all space is used or the configuration meets your requirements. Note: a small portion will be unavailable to partition. This is normal. In this example, it is 8 MB.

9. Select what format you wish to use by pressing the UP ARROW and DOWN ARROW keys.

Press ENTER to confirm your selection and Continue or ESC to Cancel.

10. Watch the progress bar as Setup formats the partition, It may take awhile.

11. After the partition is a finished formatting, Setup copy various files to support booting from the hard drive and continue on.

12. The first reboot and the end of the blue background has arrived. If you are impatient, press ENTER to Restart before the 15 seconds expire.

ENTER to Restart the Computer is the only option available.

13. The new Windows Server 2003 Family boot screen is displayed.

14. Windows Server 2003 Installation:

Sit back. It may be awhile.

15. Region and Input Languages Option

16. Enter in your Name and optional Organization information, and then select the Next button.

Select the **Next** button to continue.

17. Enter your unique 25 digit Product Key that came with your CD or download, and then select the **Next** button.

18. Configure the Licensing mode.

- Options are Per server or Per seat.
- Per server is usually used for a single-server network.
- Per client is used if all of the concurrent connections is higher than the number of clients or seats that you have.

19. Enter an Administrator Password now. It is very important that you keep this information safe and remember what it is!

Select the **Next** button to continue.

20. If the chosen password does not meet acceptable guidelines, a warning box will appear with suggestions on how to make the system more secure.

21. Configure the proper information for the Date, Time and Time Zone here.

Select the **Next** button to continue.

22. Faster development of applications, but still slow install times. Wait here while the Network is installing.

23. The Network Settings Dialog is next. Under usual circumstances, the **Typical settings** are fine.

Choose your method and select the **Next** button.

24. Custom settings for network (Network Load Balancing).

25. File and Print Sharing for Microsoft Networks has several options not available with Windows XP Home or Professional.

26. TCP/IP Properties contains the standard options. Adjust them for your particular needs as required. Select the **Advanced** button to further configure your TCP/IP options.

27. **Select** Workgroup or Computer Domain.

Select the **Next** button after making your choice.

28. Install screen appear.

The system will reboot after all files have been copied over to the install partition. Now may be a good time to take a break. It may be awhile.

29. The moment we have all been waiting for, Windows 2003 is starting up for the first time.

30. Hit the "Three Finger Salute" combination of Ctrl+Alt+Delete to login to the Administrator account.

You did remember your password, right?!?

31. Enter your password to login to the Administrator account.

Select **OK** to continue.

❖ Windows 2003 Enterprise Server Configuration:

- After installing and activating Windows, you can configure the server using the Manage Your Server page that launches automatically at logon.
- The page facilitates the installation of specific services, tools, and configurations based on server roles.
- Click Add or Remove a Role and the Configure Your Server Wizard appears.
- If you select Typical Configuration For A First Server, the Configure Your Server Wizard promotes the server to a domain controller in a new domain, installs Active Directory services, and, if needed, Domain

Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), and Routing And Remote Access (RRAS) service.

- If you select Custom Configuration, the Configure Your Server Wizard can configure the following roles:

- **Following Step required Configuring Windows 2003 :**

Example: Configure the server as the first domain controller in an Active Directory domain called contoso.com**.**

- 1. If it is not already open, open the Manage Your Server page from the Administrative Tools program group.
- 2. Click Add Or Remove A Role. The Configure Your Server Wizard appears.
- 3. Click next and the Configure Your Server Wizard detects network settings.
- 4. Click Typical Configuration For A First Server, and then click Next.
- 5. In Active Directory Domain Name, type contoso.com.
- 6. Verify that NetBIOS Domain Name reads CONTOSO and click Next.
- 7. Verify that the Summary of Selections matches that shown in Figure and click Next.

  The Configure Your Server Wizard reminds you that the system will restart and asks you to close any open programs.

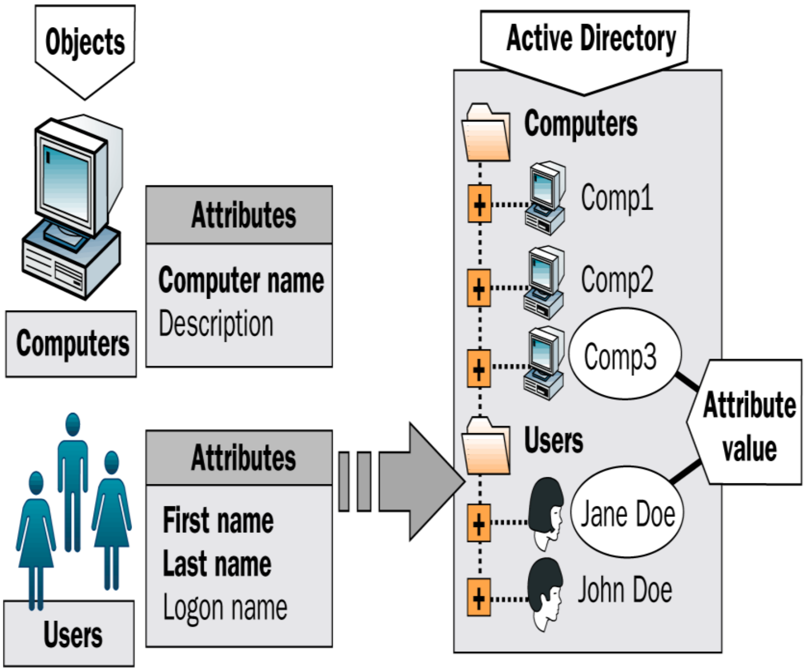
- 8. Click Yes.
- 9. After the system has restarted, log on as Administrator.
- 10. The Configure Your Server Wizard will summarize its final steps, as shown in Figure.

❖ **Active Directory :**

- Microsoft Windows networks support two directory service models:
- The workgroup
- And the domain.
- The domain model is by far the more common in organizations implementing Windows Server 2003.
- The domain model is characterized by a single directory of enterprise resources that is trusted by all secure systems that belong to the domain.
- Those systems can therefore use the security principals (user, group, and computer accounts) in the directory to secure their resources.
- **Active Directory thus acts as an identity store, providing a single trusted list of Who's Who in the domain.**
- Active Directory itself is more than just a database,
- It is a collection of supporting files including transaction logs and the system volume, or Sysvol, that contains logon scripts and group policy information.
- It is the services that support and use the database, including Lightweight Directory Access Protocol (LDAP), Kerberos security protocol, replication processes, and the File Replication Service (FRS).
- The database and its services are installed on one or more domain controllers.
- A domain controller is a server that has been promoted by running the Active Directory Installation Wizard by running DCPROMO from the command line or by running the Configure Your Server Wizard.

- Once a server has become a domain controller, it hosts a copy, or replica, of Active Directory and changes to the database on any domain controller are replicated to all domain controllers within the domain

❖ Active Directory Objects and Attributes :



❖ Active Directory Components:

Logical Structure

- Domains
- Organizational units
- Trees
- Forests

Physical Structure

- Sites
- Domain controllers

❖ Domains, Trees and Forests :

- **Domain** : Administrative unit of Active Directory
- **Tree :** A collection of one or more domains
- **Forest :** A collection of one or more trees
- Active Directory cannot exist without at least one domain.
- A domain is the core administrative unit of the Windows Server 2003 directory service.
- An enterprise may have more than one domain in its Active Directory.
- Multiple domain models create logical structures called trees when they share contiguous DNS names.
- For example **microsoft.com**, **uk.microsoft.com**, and us.microsoft.com share contiguous DNS namespace, and would therefore be referred to as a tree.
- If domains in an Active Directory do not share a common root domain, they create multiple trees.
- That leads you to the largest structure in an Active Directory: the forest.
- An Active Directory forest includes all domains within that Active Directory.

- A forest may contain multiple domains in multiple trees, or just one domain.
- When more than one domain exists, a component of Active Directory called the **Global Catalog** becomes important because it provides information about objects that are located in other domains in the forest and reduces LDAP queries to Active Directory.

❖ Managing Active Directory Objects :

- When you first install Active Directory, a number of Containers are created to hold built-in users and groups, as well as computer accounts by default
- Organizational Units (OUs) allow the assignment of Group Policy and delegation of administrative control to junior administrators
- User accounts are best arranged into Organizational Units and have certain management functions that can be delegated at the OU level and inherited by lower levels.
- **User Account :**

  A user account consists of
    - Username and password
    - Group membership
    - Rights and permissions to access resources.

  Windows Server 2003 Computer configured as a Domain Controller with Active Directory
    - User accounts are managed by Active Directory Users and computers.

  Windows Server 2003 computer member Server (not a Domain Controller) and Windows XP workstations
    - User accounts are managed by Local Users and Groups
- **Computer Account :**
- Computer accounts are created and stored in the Active Directory like User and group accounts.
- Like users and group accounts, computer accounts have their own **specific attributes or properties** by which they can be searched and identified in the Active Directory.
- They can be members of security or distribution groups and inherit permissions from group objects.
- They inherit group policy settings from container objects such as domains, sites and Organizational Units (OUs).
- Computer accounts are used to identify computers in a domain with their security principles – SID
- A user with a valid user account and a password in Active Directory cannot log on to a domain, if the computer is not represented in that domain.
- Each Windows Server 2003 computer, Windows XP, Windows 2000 Server and Professional computer, Windows NT Server and workstation computer must have a computer account in an Active Directory - Domain Controller (DC) to participate in a domain.
- Windows 95, 98, Me computers must install Active Directory Client software to participate in a domain
- Computer account password is generated automatically by the operating system and kept hidden.

- **Group Account :**
- Groups are a collection of user and computer accounts that you manage as a single unit.
- Groups simplify administration by enabling you to grant permissions to resources to the group rather that to each user individually.
- Are characterized by Scope and Type.
- Groups can be nested (groups can be members of other groups).
- In addition to user accounts, you can add other groups, contacts, and computers to groups
- Windows 2000 provides the ability to create groups:
- in a stand-alone computer security accounts database
- in Active Directory

Types of Groups:

- **Security groups :**
  - Windows 2000 itself only uses security groups, which you use to assign permissions to access resources and rights to perform tasks
  - Has all of the same functionality as distribution groups.
- **Distribution groups :**
  - Applications can use distribution groups as lists for non security-related functions

– You cannot use distribution groups to assign rights and permissions.

- **How to Create a Group :**
  - Active Directory Users and Computers Right click the OU or Container you want to create a group in and click New>>Group

❖ **Monitoring Performance :**

- One of the most important tasks that should be performed on the network is some form of statistical collecting.
- These statistics can range from the performance of servers, workstations, and other
- Devices on the network to the performance of individual components within a program or service itself.
- Generally Several types of performance monitoring tools:
  - Simple Network Management Protocol (SNMP),
  - Windows NT Performance Monitor, and
  - Windows 95's System Monitor.
- **Simple Network Management Protocol (SNMP) :**
- Many types of software and hardware on the market enable you to collect statistics on the network.
- One important protocol used within the TCP/IP protocol suite that assists in statistic collecting is the Simple Network Management Protocol (SNMP).
- SNMP is a protocol that is supported by most pieces of hardware and software that support the TCP/IP protocol stack.
- This protocol allows for the collection of statistics of various resources on the network.

  For this information to be collected about a resource, the resource must run an SNMP service, or have some other device run the SNMP service on its behalf.
- The SNMP service collects predefined information. This information is stored in a Management Information Base (MIB).

- An MIB is a database of information that can be read by management software designed to work with SNMP.

Management software issues one of the following three main commands:

. The get command gathers information within an MIB.

. The get next command gets the next piece of information within the MIB.

. The set command places information within the MIB.

- These devices that have an SNMP service monitoring them can also be configured to issue traps, or system messages, when certain parameters are reached or exceeded.

● Windows NT Performance Monitor :

- Windows NT's Performance Monitor tool lets you monitor important system parameters for the computers on your network in real-time.
- Performance Monitor can keep an eye on a large number of system parameters, providing a graphical or tabular profile of system and network trends.
- Performance Monitor also can save performance data in a log for later reference.
- You can use Performance Monitor to track statistical Measurements (called counters) for any of several hardware or software components (called objects).
- An example of these counters for an object being displayed in a chart format can be seen in Figure.

Some Performance Monitor objects that relate to network behavior are as follows:

. Network segment

. Server

. Server work queues

. Workstation or other Redirectors

. Protocol-related objects, such as TCP, UDP IP, NetBEUI, NWLink, and NetBIOS

. Service-related objects, such as Browser and Gateway Services for NetWare.

Some Performance Monitor counters that relate to the performance of components or resources on a computer are as follows:

. Processor

. Memory

. Physical Disk

❖ Monitoring Network Traffic :

- Protocol analysis tools monitor network traffic by intercepting and decoding frames.
- Software-based tools, such as Windows NT Server's Network Monitor (see Figure), analyze frames coming and going, in real time, from the computer on which they run.
  - Network Monitor records a number of statistics, including the percent of network utilization and the broadcasts per second.
  - In addition, Network Monitor tabulates frame statistics (such as frames sent and received) for each network address.

- An enhanced version of Network Monitor, which is included with the Microsoft BackOffice System Management Server (SMS) package, monitors traffic on more than just the traffic between the local computer and other devices.
- It will also monitor traffic that is just between other devices, and also traffic on remote networks, provided a monitor agent is installed on the remote network segment.
- For large networks, or for networks with complex traffic patterns, you might want to use a hardware-based protocol-analysis tool.
- A hardware-based protocol analyzer is a portable device that can be as small as a palmtop PC or as large as a suitcase.
- The advantage of a hardware-based protocol analyzer is that you can carry it to strategic places around the network (such as a network node or a busy cabling intersection) and monitor the traffic at that point.
- A hardware-based protocol analyzer is often a good investment for a large network because it concentrates a considerable amount of monitoring and troubleshooting power into a single, portable unit.
- For a smaller network, however, a hardware-based analyzer might not be worth the initial five-figure expense because less expensive software-based products perform many of the same functions.

❖ **Monitoring Network Traffic :**

- Some operating systems, such as Windows NT, have the capability to keep a running log of system events.
- That log serves as a record of previous errors, warnings, and other messages from the system.
- Studying the event log can help you find recurring errors and discover when a problem first appeared.
- The event log should also be scanned on a regular basis to look for any indications of potential problems.
- Windows NT's Event Viewer application provides you with access to the event log.
- **You can use Event Viewer to monitor the following types of events:**
- **System events:**. Warnings, error messages, and other notices describing significant system events. Examples of system log entries include browser elections, service failures, and network Connection failures.
- **Security events:** Events tracked through Windows NT's auditing features.
- **Application events**. you can check the application log for an application-related error or warning message, provided the application is programmed to write to the event log. Some NT services such as the JET database engine used by WINS record their information in the application events log rather than the system log.
- **The Windows NT Event Viewer utility contains the following five types of events:**

1. **Information.** These events simply state that something of importance has been done, such as the loading of a protocol. These events are recorded for a matter of information only.
2. **Warning.** These events serve as a warning that some event that may be important has occurred. Often when services are stopped, a warning event is generated.
3. **Stop.** These events occur when something of significance, such as a detrimental event, has occurred. Often when services or hardware fail, a Stop event is generated.
4. **Success**. This event is generated within the auditing log.
   Success events are generated when an object that was audited as
   Successful has occurred. You might, for example, audit the successful
   Logon of users.
5. **Failure.** This event is generated within the auditing log.
   Failure events are generated when an object that was audited as a
   Failure has occurred, such as the failure of users to log on.

❖ Microsoft Management Console(MMC) :

- MMC is the primary tool used to administer Windows Server 2003.
- In a Windows Server 2003 environment, administrator will normally be responsible for more than one server.
- A large number of pre-configured MMC are available in the Administrative Tools menu.
- A useful tool for administrators to manage Windows computers anywhere on the network
  (Remote server and clients) is **Microsoft Management Console (MMC)**
- MMC provides a customizable management framework for hosting multiple management tools (snap-ins)
- MMC with one or more snap-ins is called **console**
- Can add and remove management tools as necessary and save as a custom MMC console file with .msc extension
- Most of the shortcuts in the Administrative Tools program group are preconfigured MMC consoles.
- The executable file for MMC is **Mmc.exe.**
- Run this file from the Run dialog box or command prompt.
- Empty console appears, select Add/Remove snap-in from the **File** menu.
- **Select** and **add** as many stand-alone snap-ins to a console and save it as a custom console with **.msc file extension.**
- Can access a remote computer through selecting Connect to Another Computer from Action menu in the MMC snap-in.
- Also, by using Add/Remove snap in from **File** menu, selecting what computer you want to manage from the list of snap-ins and then clicking **Add** button.

UNIT- 5

Chapter 10: Network Security

❖ Fundamental of Network Security :

When you are planning, designing, or implementing a network or are assigned to operate and manage one, it is useful to ask yourself the following questions:

1. What are you trying to protect or maintain?
2. What are your business objectives?
3. What do you need to accomplish these objectives?
4. What technologies or solutions are required to support these objectives?
5. Are your objectives compatible with your security infrastructure, operations, and tools?
6. What risks are associated with inadequate security?
7. What are the implications of not implementing security?
8. Will you introduce new risks not covered by your current security solutions or policy?
9. How do you reduce that risk?
10. What is your tolerance for risk?

You can use these questions to pose and answer some of the basic questions that underlie fundamental requirements for establishing a secure network. Network security technologies reduce risk and provide a foundation for expanding businesses with intranet, extranet, and electronic commerce applications.

Solutions also protect sensitive data and corporate resources from intrusion and corruption.

Advanced technologies now offer opportunities for small and medium-sized businesses (SMB), as well as enterprise and large-scale networks to grow and compete; they also highlight a need to protect computer systems against a wide range of security threats.

The challenge of keeping your network infrastructure secure has never been greater or more crucial to your business. Despite considerable investments in information security, organizations continue to be afflicted by cyber incidents. At the same time, management aims for greater results with fewer resources. Hence, improving security effectiveness remains vital, if not essential, while enhancement of both effectiveness and flexibility has also become a primary objective.

Without proper safeguards, every part of a network is vulnerable to a security breach or unauthorized activity from intruders, competitors, or even employees. Many of the organizations that manage their own internal network security and use the Internet for more than just sending/receiving e-mails experience a network attack—and more than half of these companies do not even know they were attacked. Smaller companies are often complacent, having gained a false sense of security. They usually react to the last virus or the most recent defacing of their website. But they are trapped in a situation where they do not have the necessary time and resources to spend on security.

❖ Security Paradigm :

As the size of networks continues to grow and attacks to those networks become increasingly sophisticated, the way we think about security changes. Here are some of the major factors that are changing the security paradigm:

- **Security is no longer about "products":** Security solutions must be chosen with business objectives in mind and integrated with operational procedures and tools.
- **Scalability demands are increasing:** With the increasing number of vulnerabilities and security threats, solutions must scale to thousands of hosts in large enterprises.
- **Legacy endpoint security Total Cost of Ownership (TCO) is a challenge:** Reactive products force deployment and renewal of multiple agents and management paradigms.
- **Day zero damage:** Rapidly propagating attacks (Slammer, Nimda, MyDoom) happen too fast for reactive products to control. Therefore, an automated, proactive security system is needed to combat the dynamic array of modern-day viruses and worms.

❖ Principles of Security—The CIA Model :

A simple but widely applicable security model is the confidentiality, integrity, and availability (CIA) triad. These three key principles should guide all secure systems. CIA also provides a measurement tool for security implementations. These principles are applicable across the entire spectrum of security analysis—from access, to a user's Internet history, to the security of encrypted data across the Internet. A breach of any of these three principles can have serious consequences for all parties concerned.

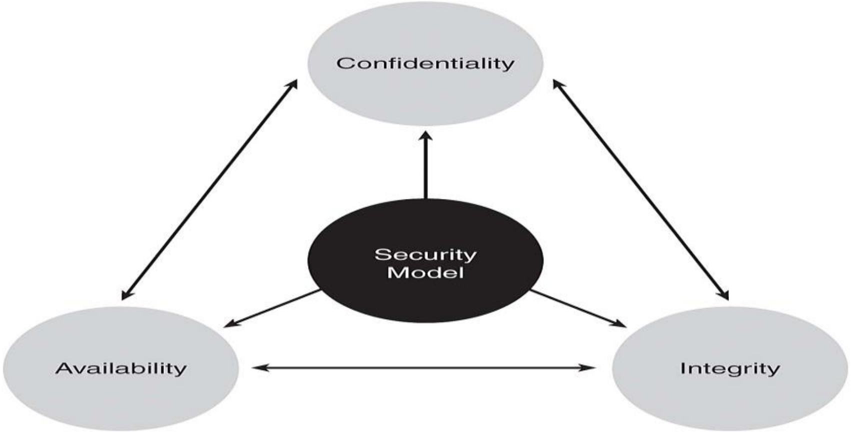


Fig: CIA Triad

Confidentiality:

Confidentiality prevents unauthorized disclosure of sensitive information. It is the capability to ensure that the necessary level of secrecy is enforced and that information is concealed from unauthorized users. When it comes to security, confidentiality is perhaps the most obvious aspect of the CIA triad, and it is the aspect of security most often attacked. Cryptography and encryption methods are examples of attempts to ensure the confidentiality of data transferred from one computer to another. For example, when performing an online banking transaction, the user wants to protect the privacy of the account details, such as passwords and card numbers. Cryptography provides a secure transmission protecting the sensitive data traversing across the shared medium.

Integrity:

Integrity prevents unauthorized modification of data, systems, and information, thereby providing assurance of the accuracy of information and systems. If your data has integrity, you can be sure that it is an accurate and unchanged representation of the original secure information. A common type of a security attack is man-in-the-middle. In this type of attack, an intruder intercepts data in transfer and makes changes to it.

Availability:

Availability is the prevention of loss of access to resources and information to ensure that information is available for use when it is needed. It is imperative to make sure that information requested is readily accessible to the authorized users at all times. Denial of service (DoS) is one of several types of security attacks that attempts to deny access to the appropriate user, often for the sake of disruption of service.

❖ Policies, Standards, Procedures, Baselines, Guidelines:

A *security model* is a multilayered framework made of many integrated entities and logical and physical protection mechanisms, all working together to provide a secure system that complies with industry best practices and regulations

Security Policy:

A *security policy* is a set of rules, practices, and procedures dictating how sensitive information is managed, protected, and distributed. In the network security realm, policies are usually point specific, which means they cover a single area. A security policy is a document that expresses exactly what the security level should be by setting the goals of what the security mechanisms are to accomplish. Security policy is written by higher management and is intended to describe the "whats" of information security.

Trust is one of the main themes in many policies. Some companies do not have policies because they trust in their people and trust that everyone will do the right thing. But, that is not always the case, as we all know. Therefore, most organizations need policies to ensure that everyone complies with the same set of rules.

A policy should define the level of control users must observe and balance that with productivity goals. An overly strict policy will be hard to implement because compliance will be minimal or ignored. On the contrary, a loosely defined policy can be evaded and does not ensure accountability and responsibility. A good policy has to have the right balance.

Standards:

Standards are industry-recognized best practices, frameworks, and agreed principles of concepts and designs, which are designed to implement, achieve, and maintain the required levels of processes and procedures.

Like security policies, standards are strategic in nature in that they define systems parameters and processes.

Standards vary by industry. There are two notable standards in security information management—ISO 17799 and COBIT.

Procedures:

Procedures are low-level documents providing systematic instructions on how the security policy and the standards are to be implemented in a system. Procedures are detailed in nature to provide maximum information to users so that they can successfully implement and enforce the security policy and apply the standards and guidelines of a security program.

Employees usually refer to procedures more often than other policies and standards because procedures provide the actual details of the implementation phase of a security program.

Baselines:

A *baseline* is the minimum level of security requirement in a system. Baselines provide users the means to achieve the absolute minimum security required that is consistent across all the systems in the organization. For example, a company might have a baseline for Windows 2000 servers to have Service Pack 4 installed on each server in the production environment. The procedure document would supplement the baseline by spelling out step-by-step instructions on where to download Service Pack 4 and how to install it to comply with this security level.

Guidelines:

Guidelines are recommended actions and operational guides for users. Similar to procedures, guidelines are tactical in nature. The major difference between standards and guidelines is that guidelines can beused as reference, whereas standards are mandatory actions in most case

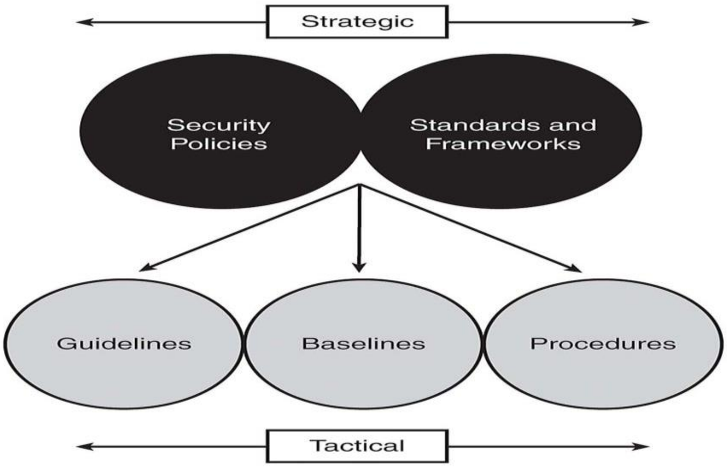


Fig.: Relationships among Security Policies, Standards, Procedures, Baselines, and Guidelines

❖ Security Models:

An important element in the design and analysis of secure systems is the security model, because it integrates the security policy that should be enforced in the system. A *security model* is a symbolic portrayal of a security policy. It maps the requirements of the policy makers into a set of rules and regulations that are to be followed by a computer system or a network system. A *security policy* is a set of abstract goals and high-level requirements, and the security model is the do's and don'ts to make this happen.

You should know about several important security models even though describing them in detail is beyond the scope of this book:

- **The Bell-LaPadula Model (BLM)**, also called the multilevel model, was introduced mainly to enforce access control in government and military applications. BLM protects the confidentiality of the information within a system.
- **The Biba model** is a modification of the Bell-LaPadula model that mainly emphasizes the integrity of the information within a system.
- **The Clark-Wilson model** prevents authorized users from making unauthorized modification to the data. This model introduces a system of triples: a subject, a program, and an object.
- The Access Control Matrix is a general model of access control that is based on the concept of subjects and objects.
- The Information Flow model restricts information in its flow so that it moves only to and from approved security levels.

- **The Chinese Wall model** combines commercial discretion with legally enforceable mandatory controls. It is required in the operation of many financial services organizations.
- **The Lattice model** deals with military information. Lattice-based access control models were developed in the early 1970s to deal with the confidentiality of military information. In the late 1970s and early 1980s, researchers applied these models to certain integrity concerns. Later, application of the models to the Chinese Wall policy, a confidentiality policy unique to the commercial sector, was developed. A balanced perspective on lattice-based access control models is provided.

❖ **ENCRYPTION**:-

→ In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor.

→ In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read 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, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors.

❖ **CRYPTOGRAPHY:**-

→ Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense.

→ The originator of an encrypted message (Alice) shared the decoding technique needed to recover the original information only with intended recipients (Bob), thereby precluding unwanted persons (Eve) from doing the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

→ Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary.

→ It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted.

→ There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.

→ The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export.

→ In some jurisdictions where the use of cryptography is legal, laws permit investigators to compel the disclosure of encryption keys for documents relevant to an investigation. Cryptography also plays a major role in digital rights management and piracy of digital media.

❖ **AUTHENTICATION**:-

→ In the context of computer systems, authentication is a process that ensures and confirms a user's identity. Authentication is one of the five pillars of information assurance (IA). The other four are integrity, availability, confidentiality and no repudiation

→ Authentication begins when a user tries to access information. First, the user must prove his access rights and identity. When logging into a computer, users commonly enter usernames and passwords for authentication purposes. This login combination, which must be assigned to each user, authenticates access. However, this type of authentication can be circumvented by hackers.

→ A better form of authentication, biometrics, depends on the user's presence and biological makeup (i.e., retina or fingerprints). This technology makes it more difficult for hackers to break into computer systems.

The Public Key Infrastructure (PKI) authentication method uses digital certificates to prove a user's identity. There are other authentication tools, too, such as key cards and USB tokens. One of the greatest authentication threats occurs with email, where authenticity is often difficult to verify. For example, unsecured emails often appear legitimate.

❖ **Perimeter Security :**

Opinions on perimeter security have changed a great deal over the past few years. Part of that change is that the very nature of perimeter security is becoming increasingly uncertain, and everyone has a different view of just what it is. The limits of the perimeter itself are becoming broad and extensive, with no geographic boundaries, and remote access is becoming part of the integral network.

Is Perimeter Security Disappearing?

In essence, the perimeter has been transformed and extended to the various levels within the network. In other words, networks today do not have a single point of entrance; they are multi-entry open environments where controlled access is required from anywhere within the network. This transformation leads us to start thinking in terms of multiperimeter networks.

The Difficulty of Defining Perimeter

Traditional networks are growing with the merging of remote network access. Wireless networks, laptops, mobile phones, PDAs, and numerous other wireless gadgets need to connect from outside the enterprise into the corporate network. To fulfill these needs, the concept of inside versus outside becomes rather complicated. For example, when you connect to the corporate network using a virtual private network (VPN), you are no longer on the outside the network. You are now on the inside of the network, and so is everything that is running on your computer.

Globally networked businesses rely on their networks to communicate with employees, customers, partners, and suppliers. Although immediate access to information and communication is an advantage, it raises concerns about security and protecting access to critical network resources.

Network administrators need to know who is accessing which resources and establish clear perimeters to control the access. An effective security policy balances accessibility with protection. Security policies are enforced at network perimeters. Often people think of a perimeter as the boundary between an internal network and the public Internet, but a perimeter can be established anywhere within a private network, or between your network and a partner's network.

❖ Security in Layers:

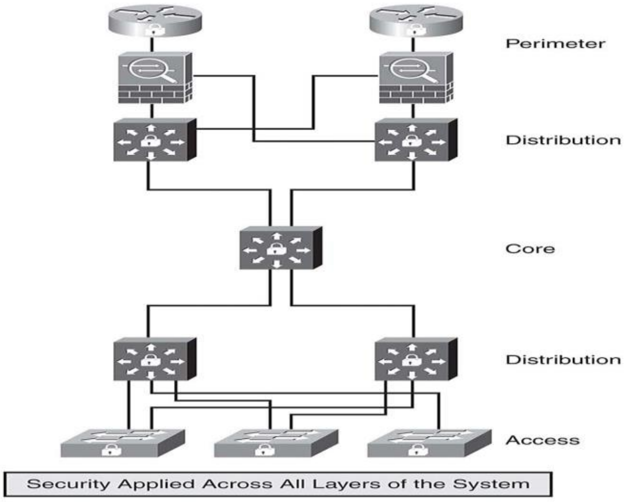
Security in layers is the preferred and most scalable approach to safeguard a network. One single mechanism cannot be relied on for the security of a system. To protect your infrastructure, you must apply security in layers. This layered approach is also called *defense in depth*. The idea is that you create multiple systems so that a failure in one does not leave you vulnerable, but is caught in the next layer. Additionally, in a layered approach, the vulnerability can be limited and contained to the affected layer because of the applied security at varying levels.

Multilayer Perimeter Solution

As stated previously, today's solutions are shifting toward the approach of placing safeguard mechanisms at various layers of the network, not just at the boundary or edge devices. Today, it is recommended to deploy Intrusion Prevention System (IPS) devices on both the inside and outside boundaries of private networks. Firewalls, on the other hand, are placed between various business segments or departments within the same organization, dividing the network into logical groupings and applying perimeter defense at each segment or department. In this multiperimeter model, each segment can have different layers of defense within it.

Effective perimeter security has become increasingly important over recent years. Perimeter security cannot be trusted to only the traditional defense mechanisms of firewalls and IDS. Web applications, wireless access, network interconnectivities, and VPNs have made the perimeter a much more complicated concept than it was a couple of years ago.

A layered approach requires implementing security solutions at different spectrums of the network. Another similar concept is *islands of security*. To implement islands of security, do not restrict your thinking to perimeter security. Do not depend on just one method for your security. You should, instead, have layers of protection—perimeter, distribution, core, and access layer. Figure illustrates a basic multilayered security mechanism, which is designed to protect the data flow in the system.



The Domino Effect

The OSI reference model was built to enable different layers to work independently of each other. The layered approach was developed to accommodate changes in the evolving technology. Each OSI layer is responsible for a specific function within the networking stack, with information flowing up and down to the next subsequent layer as data is processed. Unfortunately, this means that if one layer is hacked, communications are compromised without the other layers being aware of the problem. For example, as shown in Figure -, if the physical layer (Layer 1) was compromised, it could cause all other layers to be compromised in succession. Security is only as strong as the weakest link. When it comes to networking, any layer can be the weakest link.

❖ Security in Wheel:

Network security is a continuous process built around the corporate security policy. The security wheel depicted in Figure shows a recursive, ongoing process of striving toward perfection—to achieve a secured network infrastructure. The paradigm incorporates the following five steps:

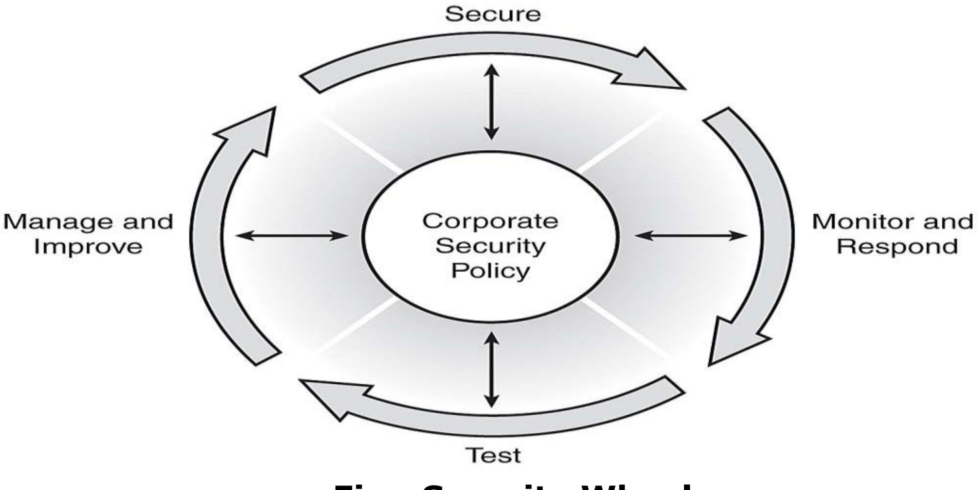


Fig: Security Wheel

Step 1: Develop a security policy

A strong security policy should be clearly defined, implemented, and documented, yet simple enough that users can easily conduct business within its parameters.

Step 2: Make the network secure

Secure the network by implementing security solutions (implement authentication, encryption, firewalls, intrusion prevention, and other techniques) to stop or prevent unauthorized access or activities and to protect information and information systems.

Step 3: Monitor and respond.

This phase detects violations to the security policy. It involves system auditing and real-time intrusion detection and prevention solutions. This also validates the security implementation in Step 2.

Step 4: Test.

This step validates the effectiveness of the security policy through system auditing and vulnerability scanning and tests existing security safeguards.

Step 5: Manage and improve.

Use information from the monitor and test phases to make improvements to the security implementation. Adjust the corporate security policy as security vulnerabilities and risks are identified. Manage and improve corporate security policy.

Lessons learned from Steps 2 through 5 should always be reflected back to the corporate security policy in Step 1, so that the high-level security expectations are being met. This should be an ongoing process, a continuous life cycle.

Chapter 11: Internet Connection and Sharing

Basic of Internet:

By the turn of the century, information, including access to the Internet, will be the basis for personal, economic, and political advancement. The popular name for the Internet is the information superhighway.

Whether you want to find the latest financial news, browse through library catalogs, exchange information with colleagues, or join in a lively political debate, the Internet is the tool that will take you beyond telephones, faxes, and isolated computers to a burgeoning networked information frontier.

The Internet supplements the traditional tools you use to gather information, Data Graphics, News and correspond with other people. Used skillfully, the Internet shrinks the world and brings information, expertise, and knowledge on nearly every subject imaginable straight to your computer.

The Internet links are computer networks all over the world so that users can share resources and communicate with each other. Some computers have direct access to all the facilities on the Internet such as the universities. And other computers, eg. Privately-owned ones have indirect links through a commercial service provider, who offers some or all of the Internet facilities.

In order to be connected to Internet, you must go through service suppliers. Many options are offered with monthly rates. Depending on the option chosen, access time may vary.

The Internet is what we call a Meta network, that is, a network of networks that spans the globe. It's impossible to give an exact count of the number of networks or users that comprise the Internet, but it is easily in the thousands and millions respectively. The Internet employs a set of standardized protocols which allow for the sharing of resources among different kinds of computers that communicate with each other on the network.

These standards, sometimes referred to as the Internet Protocol Suite, are the rules that developers adhere to when creating new functions for the Internet.

The Internet is also what we call a distributed system; there are no central archives. Technically, no one runs the Internet. Rather, the Internet is made up of thousands of smaller networks. The Internet thrives and develops as its many users find new ways to create, display and retrieve the information that constitutes the Internet.

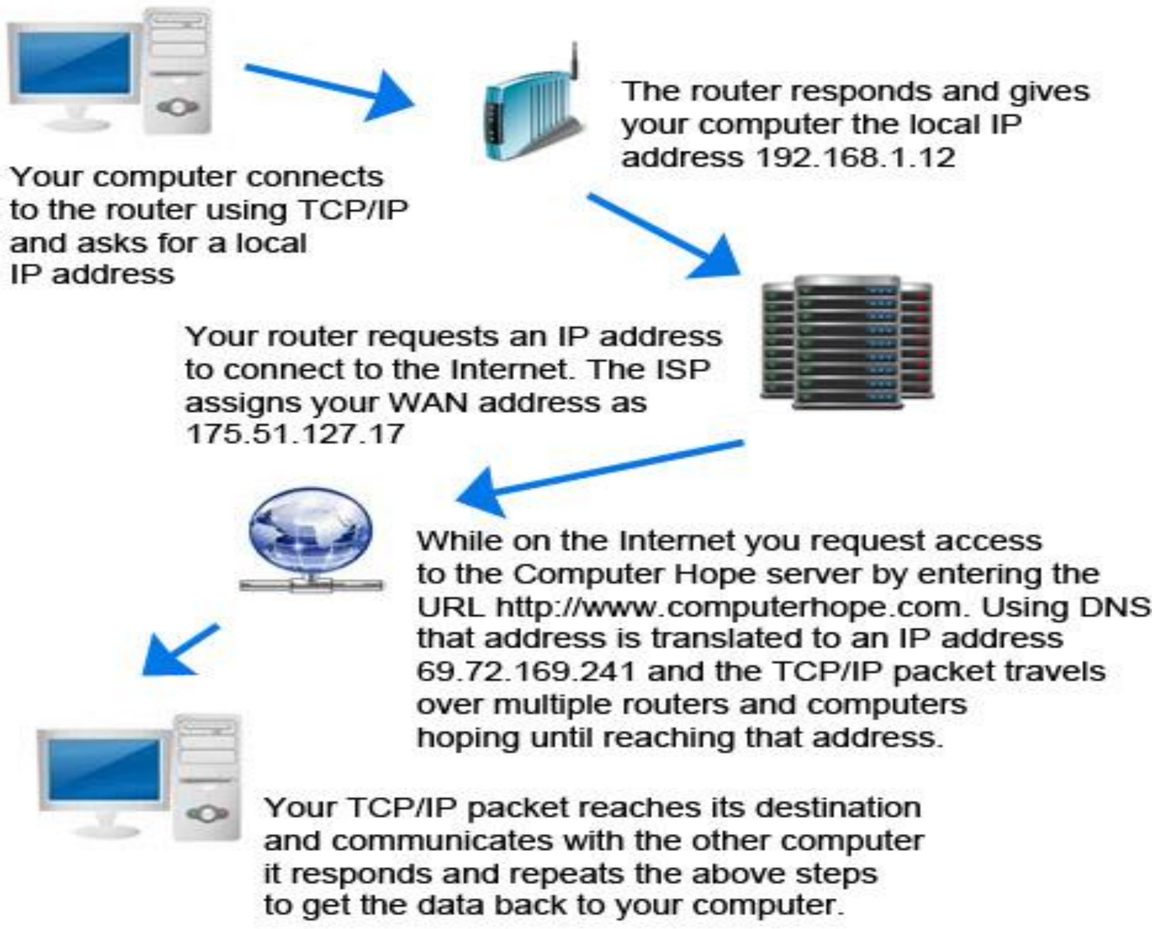
How internat is connect with computer:

Using a network connection, including connecting to the Internet, computers connect to each other to transmit data between them and communicate with each other using the TCP/IP (Transmission Control Protocol / Internet Protocol). Think of TCP/IP as a book of rules, a step-by-step guide that each computer uses to know how to talk to another computer. This book of rules dictates what each computer must do to transmit data, when to transmit data, how to transmit that data. It also states how to receive data in the same manner. If the rules are not followed, the computer will not be able to connect to another computer, nor send and receive data between other computers.

Internet service providers (ISP), the companies that provide Internet service and connectivity also follow these rules. The ISP provides a bridge between your computer and all the other computers in the world, which are all a part of the Internet. The ISP uses the TCP/IP protocols to make computer-to-computer connections possible and transmit data between them. When successfully connected to an ISP you will be assigned an IP address, which is a unique address given to your computer or network and allows it to be found while on the Internet.

If you have a home computer network, the computers are also using TCP/IP to connect to each other. This protocol allows each computer to "see" the other computers on the network and share files between them and is what makes it possible for a printer to be shared on a network. When computers connect to each other on the same network, it is called a local area network, or LAN. When multiple networks are connected to each other, it is called a wide area network, or WAN. With this type of network, your home will have a network router that connects to your ISP. The router is given the IP address for your connection to the Internet and then assigns local IP addresses to each device in your network. These local addresses are often 192.168.1.2-255. When accessing a local computer in your own network, your router sends your TCP/IP packets between the local IP addresses. However, when you want to connect to the Internet your router communicates to the Internet with the IP address assigned to it from the ISP. This is why when on the Internet your IP address is not a 192.168.x.x address.

When requesting information from a web page, such as Computer Hope you enter a URL that is easy to understand and remember. In order for your computer to access the computer containing the pages that URL must be converted into an IP address, this is done with DNS. Once DNS has converted the URL into an IP address the routers on the Internet will know how to route your TCP/IP packet. Below is a graphic illustration of everything explained above to help better illustrate the process of your computer communicating with another computer on the Internet?



Your computer connects to the router using TCP/IP and asks for a local IP address

The router responds and gives your computer the local IP address 192.168.1.12

Your router requests an IP address to connect to the Internet. The ISP assigns your WAN address as 175.51.127.17

While on the Internet you request access to the Computer Hope server by entering the URL http://www.computerhope.com. Using DNS that address is translated to an IP address 69.72.169.241 and the TCP/IP packet travels over multiple routers and computers hoping until reaching that address.

Your TCP/IP packet reaches its destination and communicates with the other computer it responds and repeats the above steps to get the data back to your computer.

Technology related internet:

.

- **Dial up Technology:**

  Definition: Dial up networking technology provides PCs and other network devices access to a LAN or WAN via standard telephone lines. Dial up Internet service providers offer subscription plans for home computer users.

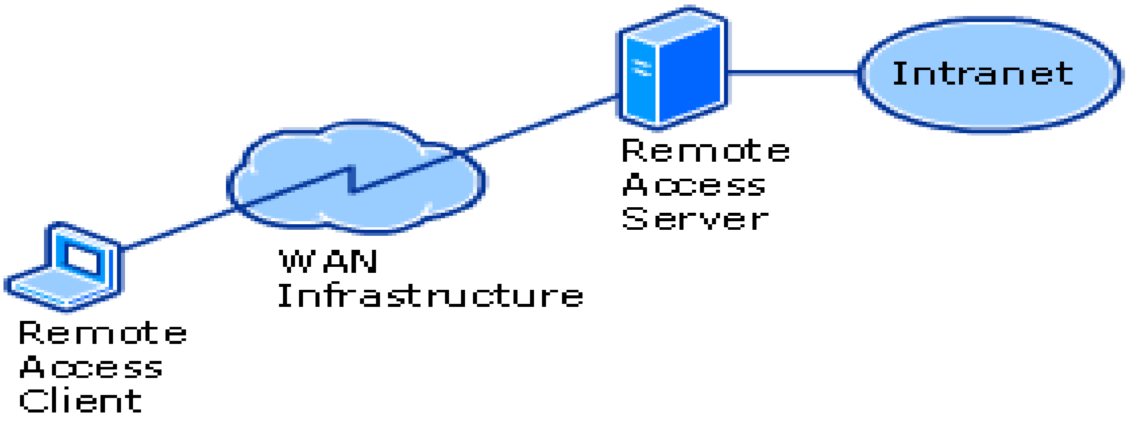
Dial-up Internet access is a form of Internet access that uses the facilities of the public switched telephone network (PSTN) to establish a dialled connection to an Internet service provider (ISP) via telephone lines. The user's computer or router uses an attached modem to encode and decode Internet Protocol packets and control information into and from analogue audio frequency signals, respectively.

The term was coined during the early days of computer telecommunications when modems were needed to connect terminals or computers running terminal emulator software to mainframes, minicomputers, online services and bulletin board systems via a telephone line.

Dial-up connections to the Internet require no infrastructure other than the telephone network. Where telephone access is widely available, dial-up remains useful to travelers. Dial-up is often the only choice available for rural or remote areas, where broadband installations are not prevalent due to low population density, and high infrastructure cost. Dial-up access may also be an alternative for users on limited budgets, as it is offered free by some ISPs, though broadband is increasingly available at lower prices in many countries due to market competition.

Dial-up requires time to establish a telephone connection (up to several seconds, depending on the location) and perform handshaking for protocol synchronization before data transfers can take place. In locales with telephone connection charges, each connection incurs an incremental cost. If calls are time-metered, the duration of the connection incurs costs. Dial-up access is a transient connection, because either the user, ISP or phone company terminates the connection. Internet service providers will often set a limit on connection durations to allow sharing of resources, and will disconnect the user—requiring reconnection and the costs and delays associated with it. Technically-inclined users often find a way to disable the auto-disconnect program such that they can remain connected for days.

A 2008 Pew Internet and American Life Project study states that only 10 percent of US adults still used dial-up Internet access. Reasons for retaining dial-up access include lack of infrastructure and high broadband prices. This has allowed Dial-up providers such as NetZero to continue spending marketing dollars to obtain customers and commit to having U.S. based customer support.



- **ISDN Network Technology (Integrated Services Digital Network)**

ISDN (Integrated Services Digital Network) is a set of CCITT/ITU standards for digital transmission over ordinary telephone copper wire as well as over other media. Home and business users who install an ISDN adapter (in place of a telephone modem) receive Web pages at up to 128 Kbps compared with the maximum 56 Kbps rate of a modem connection. ISDN requires adapters at both ends of the transmission so your access provider also needs an ISDN adapter. ISDN is generally available from your phone company in most urban areas in the United States and Europe. In many areas where DSL and cable modem service are now offered, ISDN is no longer as popular an option as it was formerly.

There are two levels of service: the Basic Rate Interface (BRI), intended for the home and small enterprise, and the Primary Rate Interface (PRI), for larger users. Both rates include a number of B-channels and a D-channels. Each B-channel carries data, voice, and other services. Each D-channel carries control and signaling information.

The Basic Rate Interface consists of two 64 Kbps B-channels and one 16 Kbps D- channel. Thus, a Basic Rate user can have up to 128 Kbps service. The Primary Rate consists of 23 B-channels and one 64 Kpbs D-channel in the United States or 30 B-channels and 1 D-channel in Europe.

ISDN in concept is the integration of both analog or voice data together with digital data over the same network. Although the ISDN you can install is integrating these on a medium designed for analog transmission, broadband ISDN (BISDN) is intended to extend the integration of both services throughout the rest of the end-to-end path using fiber optic and radio media. Broadband ISDN encompasses frame relay service for high-speed data that can be sent in large bursts, the Fiber Distributed-Data Interface (FDDI), and the Synchronous Optical Network (SONET). BISDN is intended to support transmission from 2 Mbps up to much higher, but as yet unspecified, rates.

- **Leased Line Technology:**

A leased line is a service contract between a provider and a customer, whereby the provider agrees to deliver a symmetric telecommunications line connecting two or more locations in exchange for a monthly rent (hence the term lease). It is sometimes known as a 'Private Circuit' or 'Data Line' in the UK or as CDN (Circuit Direct Number) in Italy. Unlike traditional PSTN lines it does not have a telephone number, each side of the line being permanently connected to the other. Leased lines can be used for telephone, data or Internet services. Some are ring down services, and some connect two PBXes.

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 doesn't carry anybody else's communications, the carrier can assure a given level of quality.

An internet leased line is a premium internet connectivity product, delivered over fiber normally, which is dedicated and provides uncondensed, symmetrical speeds, Full Duplex. It is also known as an Ethernet leased line, DIA line, data circuit or private circuit.

For example, a T-1 channel can be leased, and provides a maximum transmission speed of 1.544 Mbit/s. The user can divide the connection into different lines for multiplexing data and voice communication, or use the channel for one high speed data circuit. Increasingly, leased lines are being used by companies, and even individuals, for Internet access because they afford faster data transfer rates and are cost-effective for heavy users of the Internet.

- **VPN:**
  What is a virtual private network (VPN)?

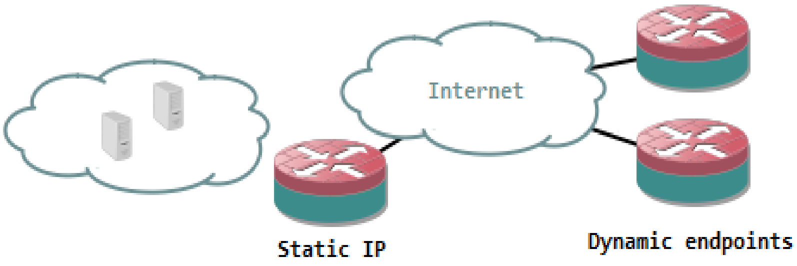
  A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.

- **Types of VPN:**

→ **Site-to-site VPN**

Often abbreviated to S2SVPN. It’s a connection between two sites and encrypts all traffic between two (or multiple) subnets. There are two types of S2SVPN:

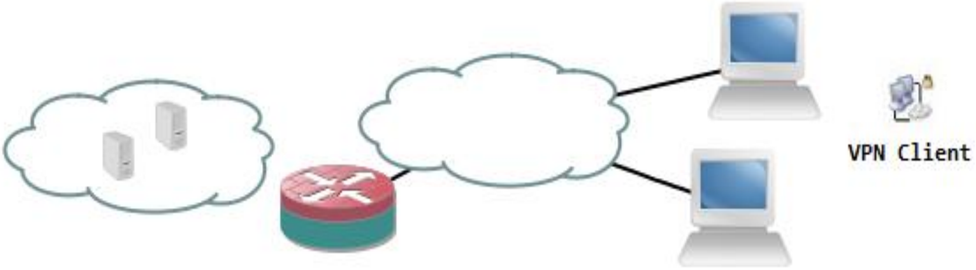
- Policy-based: interesting traffic triggers an ACL and is encrypted and sent to the remote VPN peer.
- Routed: traffic is routed into an encrypted tunnel to the remote VPN peer.
- For a detailed explanation and configuration, Jeremy made some excellent posts about this on Packetlife: Part 1 for policy-based and Part 2 for routed.



→ **DMVPN**

→ A dynamic multipoint VPN is not a protocol but more a technique using different protocols. One or more central hub routers are required, but the remote (spoke) routers can have dynamic IPs and more can be added without having to modify the configuration on the hub router(s), or any other spoke routers.

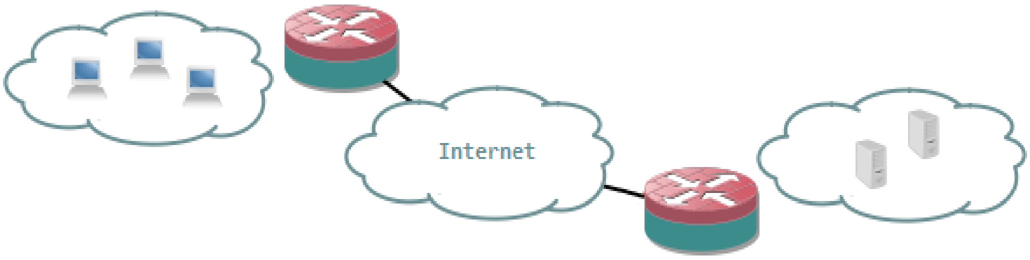
→ The routers use a next-hop resolution protocol, combined with a dynamic routing protocol to discover remote peers and subnets. The VPN itself is a mGRE tunnel (GRE with multiple endpoints) which is encrypted. This way, traffic between spoke routers does not have to go through the hub router but can be sent directly from spoke to spoke.



→ ***Different types of VPN explained.***

→ Since I'm going to talk more about VPNs in the upcoming weeks, I'm going to explain the different types of VPN here. No configuration guides, but an explanation so it's clear what is what.

→ For those who aren't sure what a VPN is: a **V**irtual Private **N**etwork is an encrypted connection between two or more devices over a public network. Some may argue that it doesn't necessarily has to be encrypted, but when it's not, that's called a tunnel (for me at least). Here's a list of the types:

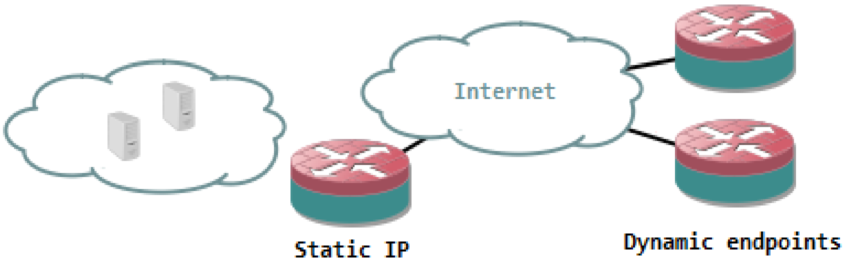


→ **Site-to-site VPN**

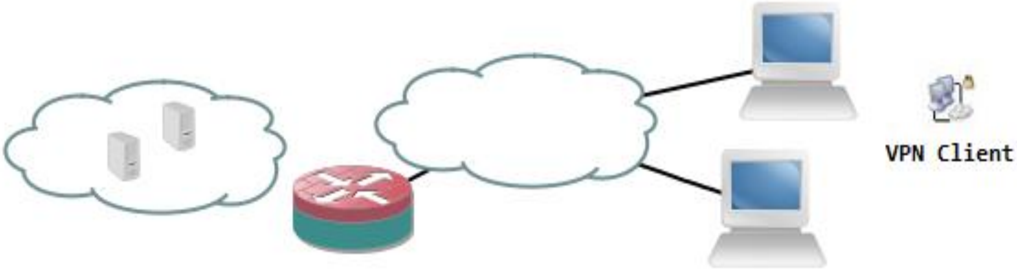
Often abbreviated to S2SVPN. It's a connection between two sites and encrypts all traffic between two (or multiple) subnets. There are two types of S2SVPN:

- Policy-based: interesting traffic triggers an ACL and is encrypted and sent to the remote VPN peer.
- Routed: traffic is routed into an encrypted tunnel to the remote VPN peer.

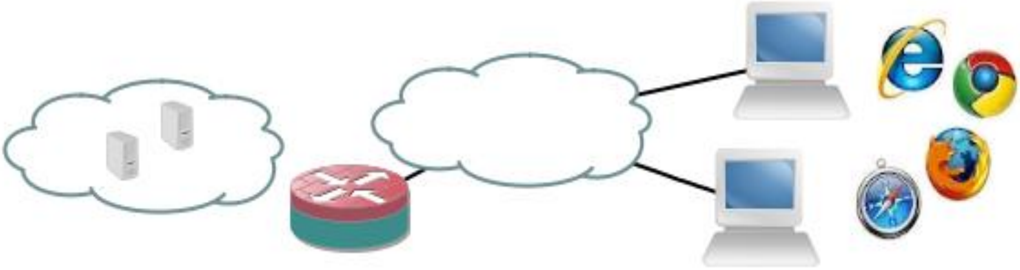
- For a detailed explanation and configuration, Jeremy made some excellent posts about this on Packetlife: Part 1 for policy-based and Part 2 for routed.



- **DMVPN**
  A dynamic multipoint VPN is not a protocol but more a technique using different protocols. One or more central hub routers are required, but the remote (spoke) routers can have dynamic IPs and more can be added without having to modify the configuration on the hub router(s), or any other spoke routers. The routers use a next-hop resolution protocol, combined with a dynamic routing protocol to discover remote peers and subnets. The VPN itself is a mGRE tunnel (GRE with multiple endpoints) which is encrypted. This way, traffic between spoke routers does not have to go through the hub router but can be sent directly from spoke to spoke.



  - **Client VPN**
    A client VPN is an encrypted connection from one device towards a VPN router. It makes that one remote device appear as a member of a local subnet behind the VPN router. Traffic is tunneled from the device (usually a computer or laptop of a teleworker) towards the VPN router so that user has access to resources inside the company. It requires client software that needs to be installed and configured.



  - **SSLVPN**
    This type of VPN works like a client VPN. The difference is that the remote client does not need preconfigured software, but instead the browser acts as VPN software. The browser needs to support active content, which every modern browser supports, either directly or through a plug-in. Traffic is tunneled over SSL (or TLS) to the SSLVPN router. From a networking perspective, traffic is tunneled over layer 4 instead of layer 3. The benefit is that the remote user does not need to

configure anything and can simply log in to a web page to start the tunnel. The drawback that you'll likely need a dedicated device as SSLVPN endpoint because this is not a standard feature.

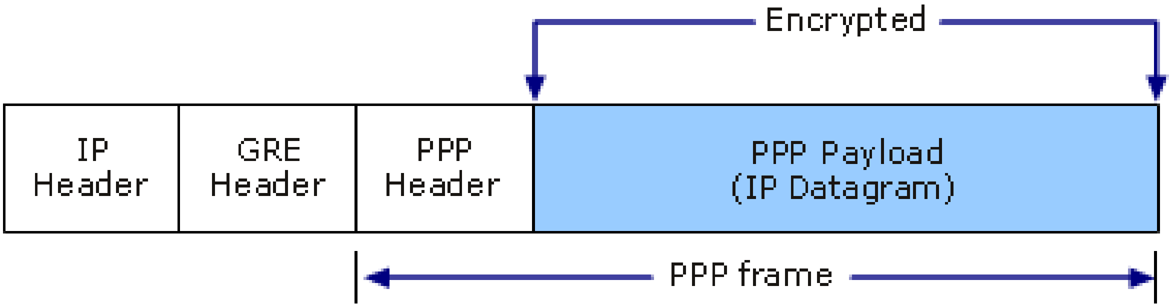
- **VPN Protocols (PPTP, L2TP, IPSec.)**
  - PPTP:

PPTP allows multiprotocol traffic to be encrypted and then encapsulated in an IP header to be sent across an IP network or a public IP network, such as the Internet. PPTP can be used for remote access and site-to-site VPN connections. When using the Internet as the public network for VPN, the PPTP server is a PPTP-enabled VPN server with one interface on the Internet and a second interface on the intranet.

Encapsulation

PPTP encapsulates PPP frames in IP datagrams for transmission over the network. PPTP uses a TCP connection for tunnel management and a modified version of Generic Routing Encapsulation (GRE) to encapsulate PPP frames for tunneled data. The payloads of the encapsulated PPP frames can be encrypted, compressed, or both. The following figure shows the structure of a PPTP packet containing an IP datagram.

Structure of a PPTP Packet Containing an IP Datagram



- L2TP

  L2TP allows multiprotocol traffic to be encrypted and then sent over any medium that supports point-to-point datagram delivery, such as IP or asynchronous transfer mode (ATM). L2TP is a combination of PPTP and Layer 2 Forwarding (L2F), a technology developed by Cisco Systems, Inc. L2TP represents the best features of PPTP and L2F.

  Unlike PPTP, the Microsoft implementation of L2TP does not use MPPE to encrypt PPP datagrams. L2TP relies on Internet Protocol security (IPsec) in Transport Mode for encryption services. The combination of L2TP and IPsec is known as L2TP/IPsec.

  Both L2TP and IPsec must be supported by both the VPN client and the VPN server. Client support for L2TP is built in to the Windows Vista® and Windows XP remote access clients, and VPN server support for L2TP is built in to members of the Windows Server® 2008 and Windows Server 2003 family.

  L2TP is installed with the TCP/IP protocol.

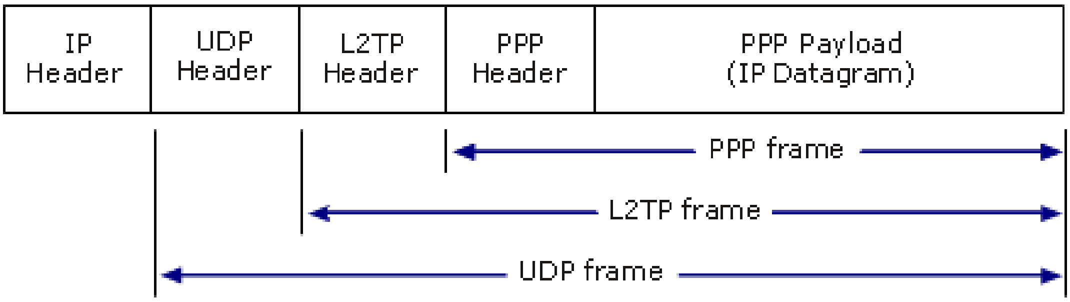
  Encapsulation

  Encapsulation for L2TP/IPsec packets consists of two layers:

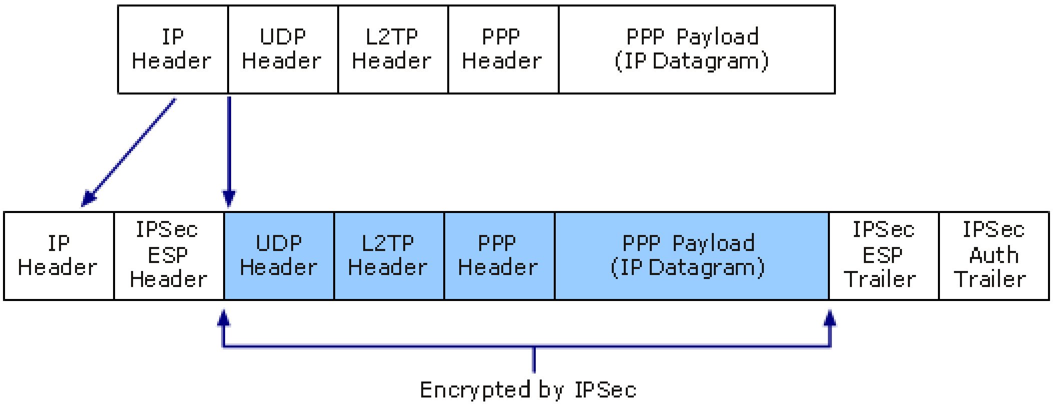
  First layer: L2TP encapsulation

  A PPP frame (an IP datagram) is wrapped with an L2TP header and a UDP header.

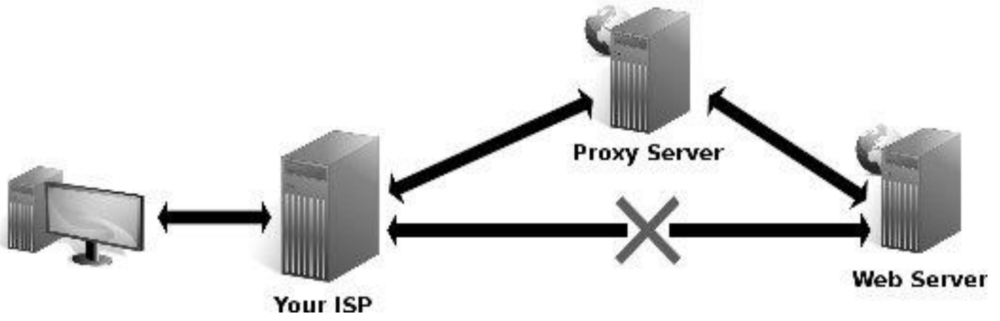
The following figure shows the structure of an L2TP packet containing an IP datagram.



Encryption of L2TP Traffic with IPsec ESP

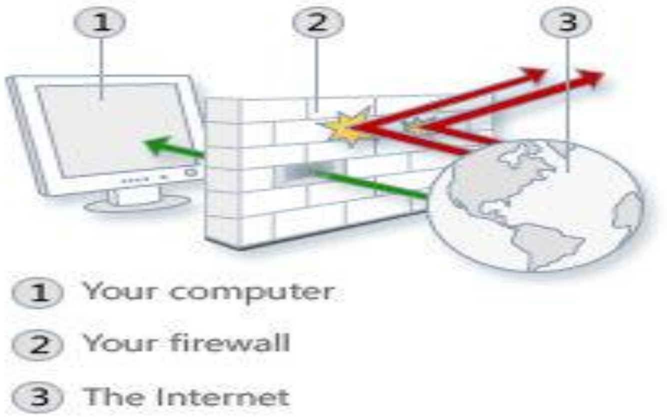


- **Proxy Server:**
During a HTTP connection, the IP address of the client machine is necessarily transmitted in order to get the information back. This allows a server to identify the source of the web request. Any resource you access can gather personal information about you through your unique IP address - your ID in the Internet. They can monitor your reading interests, spy upon you and log your requests for third parties. Also, owners of the Internet resources may impose some restrictions on users from certain countries or geographical regions.
An anonymous proxy server acts as a middleman between your browser and an end server. Instead of contacting the end server directly to get a web page, the browser contacts the proxy server, which forwards the request on to the end server. When the end server replies, the proxy server sends the reply to the browser. No direct communication occurs between the client and the destination server, therefore it appears as if the HTTP request originated from the intermediate server. The only way to trace the connection to the originating client would be to access the logs on the proxy server (if it keeps any). So an anonymous proxy server can protect your identity by stripping a request of all identifying information.



- **Firewall**

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. If you can’t start Windows Firewall or you are getting an error, use our free tool to diagnose and fix problems.



- If you use a computer at home, the most effective and important first step you can take to help protect your computer is to turn on a firewall.
- Windows 8, Windows 7, Windows Vista, and Windows XP SP2 or higher have a firewall built-in and turned on by default. (**Note:** Support for Windows XP ends in April 2014.)
- If you have more than one computer connected in the home, or if you have a small-office network, it is important to protect every computer. You should have a hardware firewall (such as a router) to protect your network, but you should also use a software firewall on each computer to help prevent the spread of a virus in your network if one of the computers becomes infected.
- If your computer is part of a business, school, or other organizational network, you should follow the policy established by the network administrator.

GPS

Global Positioning System was developed by the United States'
GPS is often used by civilians as a navigation system. On the ground, any GPS receiver contains a computer that "triangulates" its own position by getting bearings from at least three satellites. The result is provided in the form of a geographic position - longitude and latitude - to, for most receivers, within an accuracy of 10 to 100 meters. Software applications can then use those coordinates to provide driving or walking instructions.

Getting a lock on by the GPS receivers on the ground usually takes some time especially where the receiver is in a moving vehicle or in dense urban areas. The initial time needed for a GPS lock is usually dependent on how the GPS receiver starts. There are three types of start - hot, warm and cold.

The **hot start** is when the GPS device remembers its last calculated position and the satellites in view, the almanac used (information about all the satellites in the constellation), the UTC Time and makes an attempt to lock onto the same satellites and calculate a new position based upon the previous information. This is the quickest GPS lock but it only works if you are generally in the same location as you were when the GPS was last turned off.

The **warm start** is when the GPS device remembers its last calculated position, almanac used, and UTC Time, but not which satellites were in view. It then performs a reset and attempts to obtain the satellite signals and calculates a new position.

The receiver has a general idea of which satellites to look for because it knows its last position and the almanac data helps identify which satellites are visible in the sky. This takes longer than a hot start but not as long as a cold start.

And finally – the **cold start** is when the GPS device dumps all the information, attempts to locate satellites and then calculates a GPS lock. This takes the longest because there is no known information.

The GPS receiver has to attempt to lock onto a satellite signal from any available satellites, basically like polling, which takes a lot longer than knowing which satellites to look for. This GPS lock takes the longest.

In an attempt to improve lock times, cellphone manufacturers and operators have introduced the Assisted GPS technology, which downloads the current ephemeris for a few days ahead via the wireless networks and helps triangulate the general user's position with the cell towers thus allowing the GPS receiver to get a faster lock at the expense of several (kilo)bytes.

- **GPRS:**

  Definition: GPRS is a cellular networking service that supports WAP, SMS text messaging, and other data communications. GPRS technology is integrated into so-called *2.5G* mobile phones designed to provide faster data transfer speeds than older 2G cellular networks.

  General packet radio service (GPRS) is a packet oriented mobile data service available to users of the 2G cellular communication systems global system for mobile communications (GSM), as well as in the 3G systems. In 2G systems, GPRS provides data rates of56-114kbit/s.

  GPRS data transfer is typically charged per megabyte of traffic transferred, while data communication via traditional circuit switching is billed per minute of connection time, independent of whether the user actually is using the capacity or is in an idle state. GPRS is a best-effort packet switched service, as opposed to circuit switching, where a certain quality of service (QoS) is guaranteed during the connection for non-mobile users. 2G cellular systems combined with GPRS are often 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. Originally there was some thought to extend GPRS to cover other standards, but instead those networks are being converted to use the GSM standard, so that GSM is the only kind of network where GPRS is in use. GPRS is integrated into GSM Release 97 and newer releases. It was originally standardized by European Telecommunications Standards Institute (ETSI), but now by the 3rd Generation Partnership Project (3GPP). GPRS was developed as a GSM response to the earlier CDPD and i-mode packet switched cellular technologies.

- **CCTV Technology:**
  Closed-circuit television (**CCTV**) 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, or mesh 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, casinos, airports, military installations, and convenience stores. Video telephony is seldom called "CCTV" but the use of video in distance education, where it is an important tool, is often so called.[1][2]
  In industrial plants, CCTV equipment may be used to observe parts of a process from a central control room, for example when the environment is not suitable for humans. CCTV systems may operate continuously or only as required to monitor a particular event. A more advanced form of CCTV, utilizing digital video recorders[3] (DVRs), provides recording for possibly many years, with a variety of quality and performance options and extra features (such as motion-detection and email alerts). More recently, decentralized IP-based CCTV cameras, some equipped with megapixel sensors, support recording directly to network-attached storage devices, or internal flash for completely stand-alone operation. Surveillance of the public using CCTV is particularly common in many areas around the world