Unit -1
Basics of Network

❖**Network Concepts:**

➢

What is network?

- "A Network is a connection between at least two computers so that they can share resources".
- "A Computer network is defined as two computers that are linked together through either a physical cable, or a wireless device."
- A computer network is simply referred to as a network, is a collection of hardware components and computers interconnected by communication channels that allow sharing of resources and information.
- A network therefore is a set of interconnected system with something share. The shared resources can be data, a printer, a fax, modem or services such as a database or email system,
- The individual system must be connected through a pathway called "Transmission media", i.e. used to transmit resources or services between the computers.
- All the system and path way follow a set of common rules, these rules are called "protocols".
- So, as a all network must have following:
    - A resource to share (Resource)
    - A pathway to transfer data (Transmission media)
    - A set of rules (Protocols)
    - A message or data to transfer
- Objective of network:
    - Resources sharing are most common objective for providing networks within the constraints of cost and reliability of transmission link.
    - To provide communication among users.
    - To increase the reliability of processing capacity through backup and redundancy.
    - To provide centralized management and allocation of resources.
    - To provide network users with maximum performance and minimum cost.
- Advantages of network:
    - Sharing Files
    - Sharing Printers and other devices
    - Speed
    - Security
    - Email
    - Workgroup computing

❖Network Model:

- Networks generally fail into one of two broad categories, those are:
    - Client-Server networks
    - Peer-to-peer networks

➢

Client/Server Network:

- A client/server network consist a group of PCs, which consist of client and server.
- Client is the PCs which input data from the user and request a particular process from server and Server provides services.
- The primary function of client /server in simple terms: the client requests services from server, and server responds by providing those services.

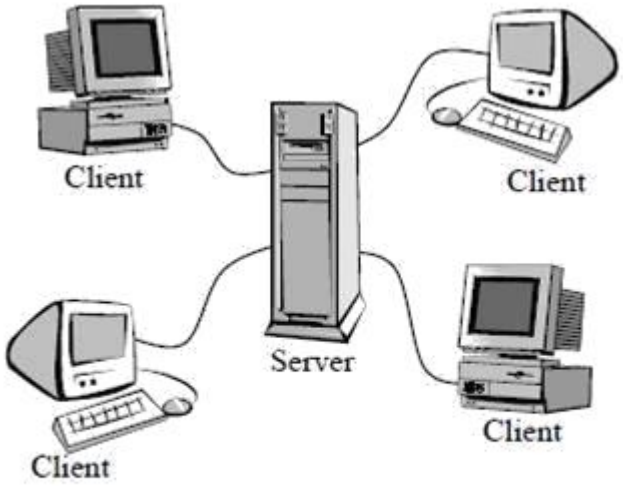


Fig-1: Client/Server Network

- Some Characteristics of Client:
    - Always initiates requests to servers.
    - Waits for replies.
    - Receives replies.
    - Usually connects to a small number of servers at one time.

- Some characteristic of server:
    - Always wait for a request from one of the clients.
    - Serve clients requests then replies with requested data to the clients.
    - Faster CPU
    - More Memory

➢Peer-to-Peer Network (Work Group):

- A peer-to-peer network is a group of users oriented PCs.
- Each Pc is called peer and these PCs operate equally.
- There is no concept of server.
- The PCs share resources such as file and printer.
- Each PC acts as both client and server.

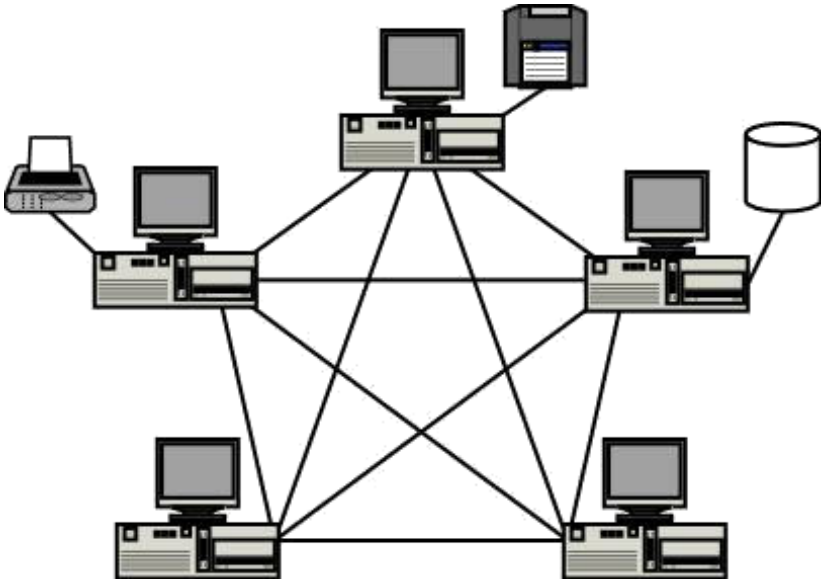


Fig-2: Peer-to-Peer Network

- Peer-to-Peer is useful for small network usually 10 machines.
- In Peer-to-Peer network the resources of any computer on the network – disk drives, files, applications, printers, modems, and so on –can be shared with any other computer.
- A Peer-to-Peer is also called workgroup.

- Advantages of Peer-to-Peer network:

    - No need of server
    - Work efficiently for smaller organization
    - Low cost
    - Easy to manage

- Disadvantages of Peer-to-Peer network:

    - Not efficient in large organization
    - Users are responsible for their own security
    - The additional load of sharing resources on computer

❖Network Services:

- Network services are the basic reasons for which we connect computers.
- There are several types of computer services such as:
  - File services
    - File transfer services
    - File storage services ○

  Print services
    - Email
    - Voice mail
    - Fax
  - Communication services
  - Database services
  - Security services
  - Application services

➢

File Services:

- File services enable networked computers to share files with each other. File services include all network function dealing with the storage, retrieval or movement of data files.
- File services enable users to read, write and manage files and data.
- File services can be centralized or decentralized. In centralized file services all files are stored in the server and in decentralized file services the entire files are stored individual most in the client.

  - File transfer Services:
    - File transfer is possible with a network using communication system.
    - For file transfer and management, file servers other purpose like security of document and backup.

  - File Storage Services:
    - Centralized storage has “online storage” hard disk.
    - In online storage data is stored on hard disk that is accessible on demand.
    - Another common approach to file storage is offline storage, which consist of removable media such as tape or an optical disk that are managed manually.

➢

Print Services:

- Many Users can share the same printers.
- This capacity is especially useful with expensive devices such as color printers and plotters.
- Printer can be located anywhere, not just next to users PC.
- Queue based network printing is more efficient then direct printing.
- Modern printing services enable user to send fax transmission through the network to fax server.

➢ Communication Services:

- Message/Communication services generally transfer information from one place to another
- This communication services is divided into sub areas,
  - Email
  - Voice Mail
  - Fax Services
- **Email**: Email system can service any size, group or term. Email also can be routed to and receive from the Internet.
- **Voice Mail:** Voice mail enables you to connect your computer to a telephone system and to incorporate telephone voicemail message with your PC. The technically term for this is "telephony".
- **Fax Services:** A Fax service enables you to send or receive faxes from your computers. This is similar to printing. You can print the document to a fax device.

➢ Database Services:

- Database services are the most common type of application servers.
- Database server provides database security.
- Optimize the performance of the database operations.
- It manages the database files by adding, deleting and modifying records solving queries and hence providing the required data by client.
- Distributed data across multiple database services.

➢ Security Services:

- Another main service which provided by network is the security services.
- Security is one of the most important elements involved in finalizing network.
- When users share resources and data on the network, they should be able to control for their own data that who can use their data or who cannot.
- Element of network security are:
  - Authentication
  - Access Permission
  - Protection and password
- A user must provide a user name and password to gain access to the system.

➢ Application Services:

- Application services enable application to leverage. The computing powers an specialized capabilities of other computers on network.
- 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 and groupware servers and directory servers.

Network Topology:

- A Topology is defined as the arrangement of nodes, cable, connectivity devices that make up the network.
- Topology are divided into two categories:
  - **Physical topology:** It describes that actual layout of transmission media.
  - **Logical topology:** It describes the logical pathway a signal follows as it passes among the network nodes.

Bus Topology:

- Bus topology is also known as linear bus.
- **In a bus topology all devices are connected to a common shared cable backbone.**
- All the node and printer are connected to backbone.
- Only one computer at a time can send message.
- It is suitable with small network.
- Most of the bus topology broadcasts signals in both directions on the backbone, so all the devices can directly receive the signals.
- A special connector called the terminator must be placed at the end of the cable to restrict data bouncing and interference from another network.

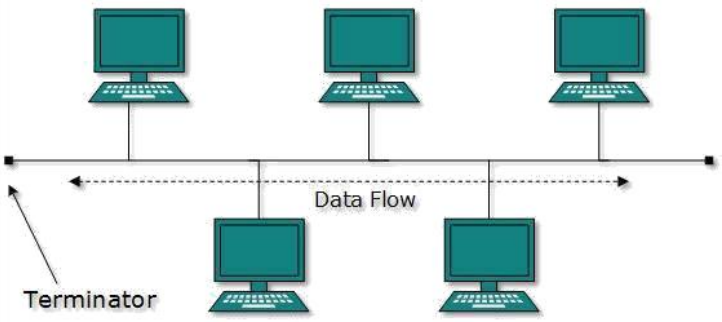


Fig-3 Bus Topology

- Advantages:
  - Easy to connect
  - Required less cable length
  - Addition of new computer is easy
  - Maintenances cost is less
- Disadvantages:
  - If Main cable break entire network will shuts down
  - Terminals are required both the sides
  - Multiple computers cannot share data at a time.
  - Difficult to find problem
  - Increase computer then communication speed will slow down.

Ring Topology:

- **In a ring topology all the nodes are wired in a circle, so it looks like a ring.**
- **Each node is connected to its neighbors on either side and data passes around the ring in the one direction**.
- Ring topologies are ideally suitable for token-passing access method.

- A token passing around the ring topology and only the node that holds the token can transmit the data.

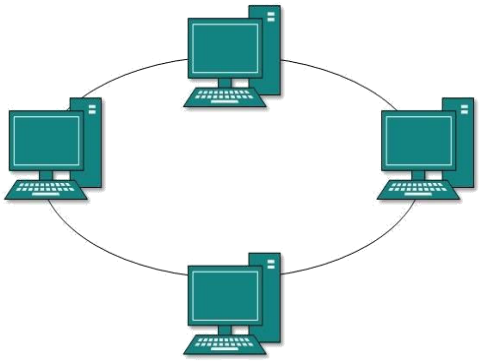


Fig-4 Ring Topology

- Advantages:
  - Network works well because there is no central computer system.
  - It is truly distributed data processing system
  - More reliable than a star network because communications is not dependent on a single host.
- Disadvantages:
  - Addition of new computer in network, increase the communication delay
  - Ring network is not popular as star network
  - Only share data between two computers, other nodes must be waiting.

➢

Star Topology:

- In star topology all devices are connected to a central hub.
- **The hub receives signal from other network devices and routes the signal to the proper destination.**
- The hub can be active or passive
- The active hub regenerates the electrical signal and send it to the all the computers connected to it.

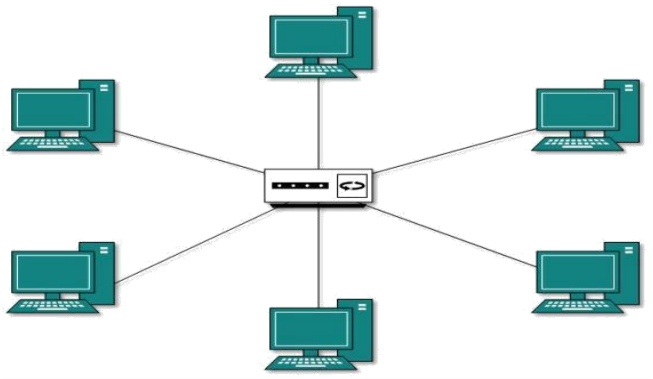


Fig-5 Star Topology

- Advantages:
  - Easy to install and remove computers
  - Easy to detect faults
  - Communication delay will not increase by adding two nodes
  - If one node fails will affect to entire network
- Disadvantages:

- Required more cable then bus network
- If central device (HUB) fails then entire network failure
- More expensive then bus topology (hub, switches)

Mesh Topology:

- **A Mesh configuration has links between each device in the network.**
- It is suitable in small network.
- In a small network you can easily troubleshoot it.

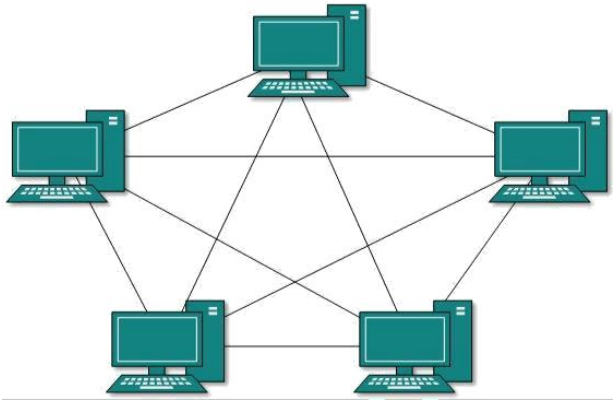


Fig-6 Mesh Topology

- Advantages:
  - If any line will breakdown will effect only communication between the connected computers
  - Communication is very fast
  - Various routes available, if one rout fails then data communicate with other routes
- Disadvantages:
  - It is most expensive network from the point of view of line cost
  - Addition of new node is difficult
  - Maintenance cost is high

Tree Topology:

- Tree Topology integrated multiple star topologies together onto bus topology.
- **A tree topology combines the characteristics of bus and star topology.**
- Tree topology allows for the expansion of an existing network.

- Advantages:
  - Point to point wiring for individual segment
  - Supported by several hardware and software
- Disadvantages:
  - If backbone line breaks then entire network fails
  - More difficult installation then other topology
  - Length of each segment is limited
  - Network expansion is difficult and does not provides speed

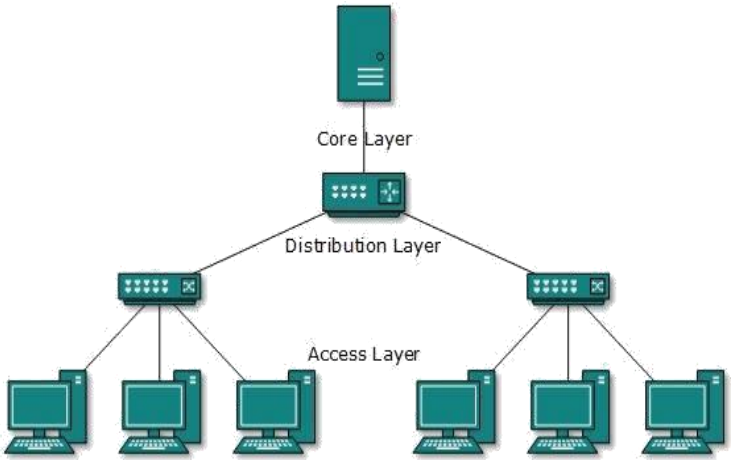


Fig-7 Tree Topology

➢ **Hybrid Topology:**

- **Hybrid network use a combination of two or more topology in such a way that the resulting network does not exhibit one of the standard topology.**
- Hybrid topology is always produced when two different basic network topology are connected.

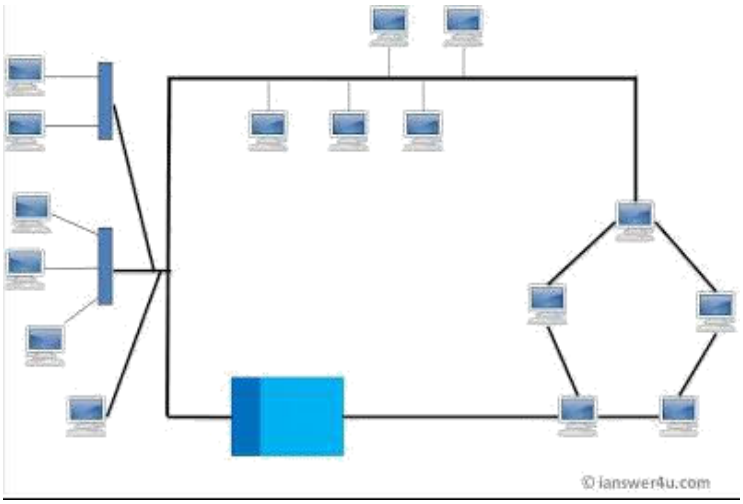


Fig-8 Hybrid Topology

- Advantages:
  - Reliability of entire system
  - Availability of Communication lines
  - Expandability of System
- Disadvantages:
  - Complexity of Design
  - Costly Hub
  - Costly Maintenance

❖ Advanced Network Topology:

➢ Ethernet:

- It was designed by Bob Metcalfe in 1973, and through the efforts of **D**igital, **I**ntel and **X**erox (for which Metcalfe worked), "DIX" Ethernet became the standard model for LANs worldwide Specified in a standard, IEEE 802.3.
- **"Ethernet is a system for connecting a number of computer systems to form a local area network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems."**
- Ethernet uses the CSMA/CD access method to handle simultaneous demands. It is one of the most widely implemented LAN standards.
- With Ethernet, file sharing and printer sharing among machines became possible.
- Ethernet is high-bandwidth technology used for internet access and connectivity by government, business and academic LANs.
- Fast Ethernet or 100BASE-T provides transmission speeds up to 100 megabits per second.
- Gigabit Ethernet provides an even higher level of backbone support at 1000 megabits per second.
- A newer version of Ethernet, called *100Base-T* (or *Fast Ethernet),* supports data transfer rates of 100 Mbps. And the newest version, Gigabit supports data rates of 1 gigabit (1,000 megabits) per second.

➢ FDDI (Fiber Distributed Data Interface) :

- Short for Fiber Distributed Data Interface, FDDI is a standard developed by the American National Standards Institute (ANSI).
- **"FDDI is an optical data communication standard used for long distance networks provides communication with fiber optic lines up to 200 kilometers at a speed of 100 megabit per second (Mbps)."**
- FDDI is developed for transmitting data on optical fiber cables.
- Topology: Dual Ring Topology
- Speed: 100 Mbps or higher
- Media: Fiber Optic cable, also possible in Copper Wire as CDDI
- Access Method: token-passing access method

➢ CDDI (Copper Data Distribution Interface):

- Copper data distribution interface (CDDI) is an implementation of fiber distributed data interface (FDDI) networking.
- CDDI is also known as Twisted Pair Distributed Data Interface (TP-DDI).
- CDDI uses cabling, which is unshielded twisted pair cables (UTP) made of copper.
- **CDDI also uses the same protocols and constructs as FDDI, but uses copper wire as the medium**.
- The logical topology used in CDDI is a ring based token network.
- CDDI is commonly implemented in a wide geographical network.
- CDDI/FDDI was considered a good system for implementing a campus network backbone in the early to mid-1990s. However, it has overcome by Ethernet and then Gigabit Ethernet.

❖Network Access Methods:

- 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 mail problem here is how different nodes get controls of the medium to send data.

  - CSMA/CD
  - CSMA/CA
  - Token Passing
  - Polling

➢CSMA/CD (Carrier Sense Multiple Access / Collision Detection) :

The most common access method in use on LANs today is CSMA/CD, which stands for Carrier-Sense Multiple Access/Collision Detection.

- **Carrier-Sense**: This means on each computer on the network "listens" and senses whether there is traffic on the cable before sending data.
- **Multiple Accesses**: This means all computers have access to the cable at any given time.

Collision Detection: This means that collisions may occur, if two computers send data at exactly the same time—but the sending computers will detect that a collision has occurred so they can re-send their data.

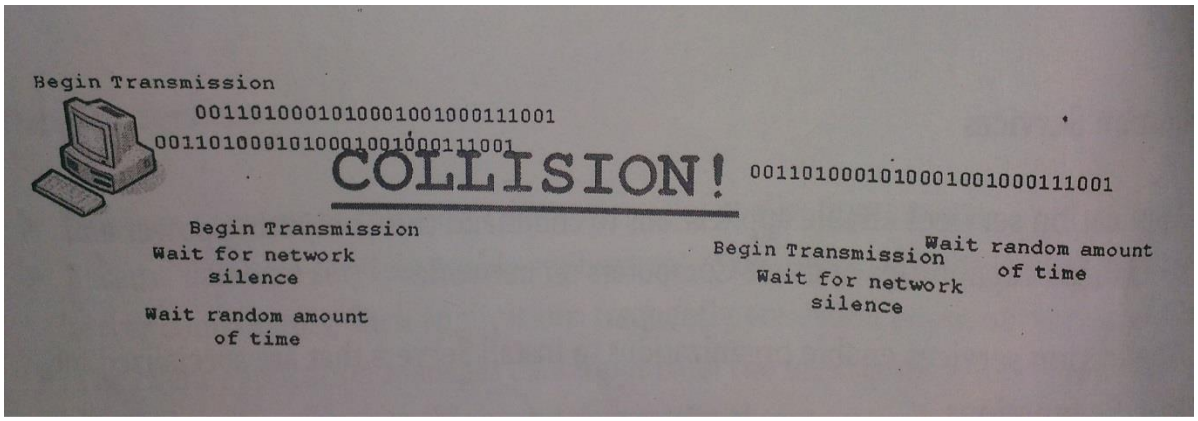


Fig-9 CSMA/CD

- Every host has equal access to the cable and can place data on the cable when the cable is free from traffic.
- When a host wants to place data on the cable, it will "sense" the cable to find whether there is a signal already on the cable.
- If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium.
- But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data.
- If the data is destroyed during transmission, the data will need to be re-transmitted.
- After collision, each host will wait for a small interval of time and again the data will be retransmitted, to avoid collision again.

➢CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) :

- It Stands for Carrier Sense Multiple Access / Collision Avoidance.
- Each device listens to media for transmissions. When transmission is clear, device sends intent to transmit signal.
- As signal is small, chances of collision are minimized.
- Used often in wireless networking.

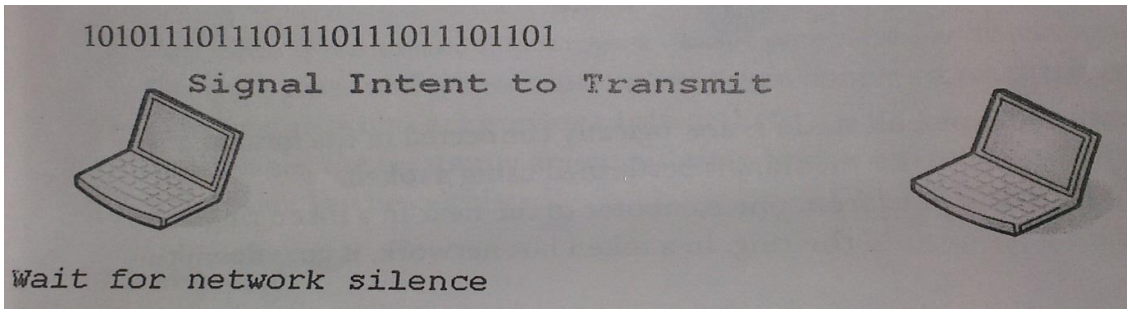


Fig-10 CSM/CA

- CSMA/CA is a media access method used in Apple's talk networks.
- CSMA/CA operates at the media-access-control (MAC) sub layer, as defined by the IEEE of the data link layer in the OSI model.
- When node wants to transmit on the network, the node listens for activity.
- If there is activity, the node waits a period of time and then tries again to access the network.

➢Token Passing:

- In Token passing 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 signal called a token goes from one computer to the next in a token ring network, the token goes around the ring. In a token bus network, it goes down the line of the bus.
- The token is passing around the network and every station check whether the message is intended for it.
- The receiving station copied the message from the token but the passes unchanged token along the network.
- When transmitting station received the same token it knows the message have been passed.

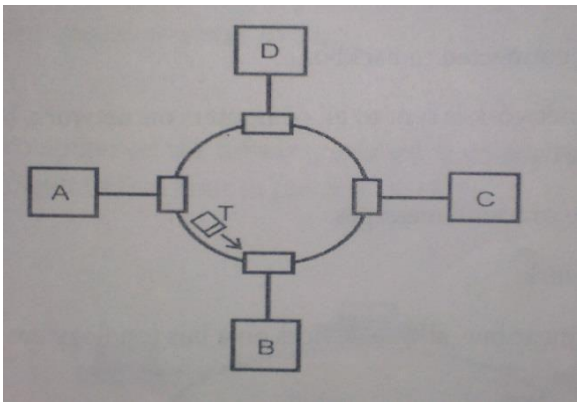


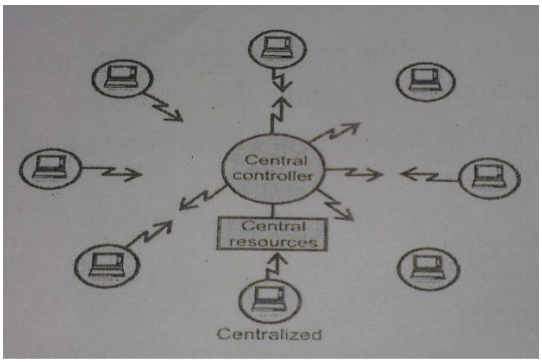
Fig-11 Token Ring Network

- Then the transmitting station erases the message and put empty token back into the network.
- If a computer has data to transmit, it must wait until the token reaches it, then that computer can capture the token and transmit data.
- A token ring network allows only one token on the cable at a time.
- There are two approaches token passing available,
    - Token Ring uses a ring topology. Each station passes the token to the next station on the ring.
    - Token Bus also uses token passing. With token bus, each station passes the token to the station with the next higher node address.

- Advantages:
    - Non-contention method. Computer do not compare for access to the cable. Each computer will get its "turn" as the token comes around the networks.
    - Effective, collisions are prevented altogether.
    - Dependable, the maximum amount of the time before a given computer will be able to transmit can be calculated.
- Disadvantage:
    - Slow, a large amount of network bandwidth is consumed in the process.
    - Costly, implementation is expensive due to the media and equipment used.

➢ Polling:

- Polling is the method of controlling the access to a transmission medium which is shared by a number of stations.
- A station user requesting service.
- The basic feature of a polling network lies in the action of the central control computer in polling each of the station on the network in a pre-specified cycle order to provide access to the communication channel.
- The message contains the address of the node being selected for granting access.
- The line containing the station and the central computers are usually high speed lines.
- Transmission between stations takes place through the central computer, which receives packet from each station and transmits them to the appropriate station.
- Roll-Call Polling:
    - The Polling sequence is based on a list of elements available the controller or poller.
- Hub Polling:
    - Each element simply polls the next element in the sequence.



Fit-12 Hub Polling

❖Communication Methods :

- There are generally 3 methods of Communication,
  - Unicasting
  - Broadcasting
  - Multicasting

➢Unicasting:

- Unicast is a communication between a single sender and a single receiver over a network.
- **"Unicast transmission is the sending of messages to a single network destination identified by a unique address."**
- Unicast transmission, in which a packet is sent from a single source to a specified distribution.
- One-to-one connection between the client and the server.
- TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) protocols are mostly used in unicast transmission method.

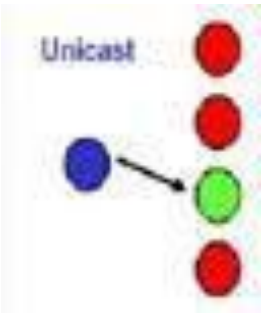


Fig-13 Unicast

➢Broadcasting:

- Broadcasting is the term used to describe communication where a piece of information is sent from one node to all other nodes.
- In this case there is just one sender, but the information is sent to all connected receivers.
- Broadcast transmission is supported on most LANs and may be used to send the same message to all computers on the LAN users.
- Network Layer Protocol (Such as IPv4) also supports broadcast that allows the same packet to be sent to every system in a logical network.
- For example: radio and TV stations.

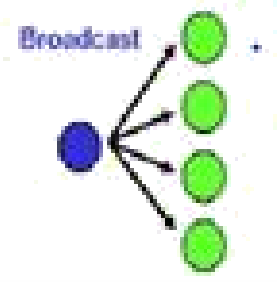


Fig-14 Broadcast

➢Multicast:

- To transmit a single message to a select group of recipients.
- Multicast is sometimes also incorrectly used to refer to a multiplexed broadcast.
- Multicast is the delivery of a message or information to a group of destination computers simultaneously in a single transmission from the source.
- A simple example of multicasting is sending an email message to a mailing list.

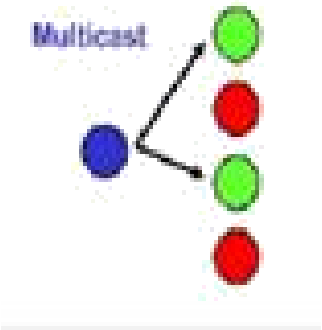


Fig-15 Multicast

❖List of Full Form

1) P2P : Peer-To-Peer
2) CDDI : Copper Data Distribution Interface
3) FDDI : Fiber Distributed Data Interface
4) TP-DDI : Twisted pair Distributed Data Interface
5) LAN L Local Area Network
6) CSMA/CD : Carrier Sense Multiple Access / Collision Detection
7) CSMA/CA : Carrier Sense Multiple Access / Collision Avoidance

Network Models and LAN Sharing

❖OSI Reference Model:

- OSI = Open System Interconnection.
- Developed by ISO (International Standard Organization) in 1984.
- OSI model refer how data should be transmitted between any two points in a telecommunication network.
- The model called ISO OSI reference model because it deals with connecting open systems-that is, systems that are open for communication with other system.
- This model has 7 layers that show how applications running upon network-aware devices may communicate with each other.
- Each layer should perform a well-defined function.
- 7 layers are,
- **A –** Application **P-** Presentation **S-** Session **T-**Transport **N-** Network **D-** Data link **P-** Physical
- To remember this layers as, All People Seem To Need Data Processing.

Application Layer

- Application layer interact with application programs and is highest level of OSI model.
- The application layer contains a variety of protocols that are commonly needed by users.
- Application protocols are used for file transfer, electronic mail and network news.
- Applications such as:
  - File Transfer
  - Email
  - Web
- Protocols used in this layer:
  - HTTP
  - SMPT
  - FTP

Presentation Layer

- This layer may translate data from a format used by the application layer into a common format.
- The presentation layer is concerned with the syntax and semantics of the information transition.
- In order to make it possible for computers with different data representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used "on the wire".
- The presentation layer manages these abstract data structures and allows higher level data structures to be defined and exchanged.
- This layer also handles data compression and data encryption.
- Data encryption:
  - Encrypt data for security purposes. For example, password encryption.
- Character code translation:
  - For example, ASCII to EBCDIC.

Session Layer

- Session layer provides mechanism for controlling the conversation between the two end systems.
- Session offers various services, including dialog control, token management and synchronization.
- It defines how to start control and end conversations between applications. (Session)
- Any necessary log-on or password validation is also handed by this layer.
- This layer Provides services like Full Duplex Or Half Duplex
- Half Duplex:
  - Handle two way data transfers in which the data flows in only one direction at a time.
  - Example:
    - Walky-talky
- Full Duplex:
  - They permit two way simultaneous data transfers by providing each device with a separate communication channel.
  - Example:
    - Telephone

Transport Layer

- The basic function of transport layer is to divide/split data into smaller unites, and pass these to the network layer, and ensure that the pieces all arrive correctly at the other hand.
- Transport layer is a true end-to-end layer, all the way from the source to the destination.
- This Layer Provides Transparent Transfer of data between two hosts means data should be error free and flow control.
- This Layer provides a reliable mechanism for the exchange of data between two processes in different computers.
- Data are divided into smaller part called segment.
- Ensure that data are delivered error-free.
- Ensure that data unites are delivered in sequence.
- Ensure that there is no loss or duplication of data.
- Protocols used in this layer are,
  - TCP (transmission Control Protocol)
  - UDP (User Datagram Protocol)

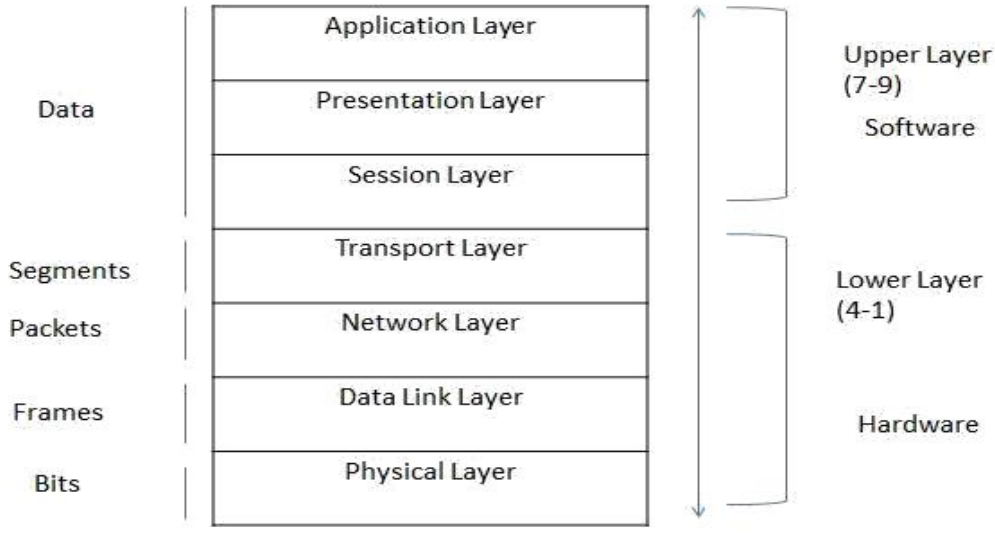


Fig 2.1-OSI reference model

Network Layer

- The network layer controls the operation of the subnet.
- A key design issue is determining how packets are routed from source to destination.
- Routes can be based on static tables that are "wired into" the network.
- It also determines the route from the source to destination computer and manages traffic.
- It defines the logical addressing so that any end point can be identified.
- Defines the best possible path the packet should be taken from the source to destination.
- Data are called Packets.
- Protocols used in this layer are,
  - Routing Protocols
  - BGP

Data Link Layer

- Data are called Frames.
- This layers responsible transferring Frames from one computer to another without any error.
- Breaks the outgoing data into frames and reassemble the received frames.
- Supports Point-to-point and broadcast communication.
- If service is reliable, the receiver confirms correct receipt of each frame by sending back an acknowledgement frame.
- Data link layer dealing with transmission errors.
- Providing the well-defined services interface to the network layer.
- Protocols used in this layer are,
  - Sliding Window Protocol
  - PPP
  - SLIP
  - Stop-and-wait Protocol

Physical Layer

- Describes the Physical and electric specification of devices.
- The physical layer is concerned with transmitting raw bits over a communication channel.
- The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit.
- Data are called Bits.
- Cable connections, Hub, repeaters
- Protocols used in this layer are:
  - 802.11
  - Ethernet
  - FDDI

TCP/IP Reference Model:

- The TCP/IP protocol was developed by the United States Department of Defense (DoD) provides high speed data communication between variety of computer types.
- TCP (Transmission Control Protocol) is used for transmit of data from an application to network. TCP is used to braking data into packets before they send to the network.

- IP (Internet Protocol) takes care of the communication with other computers. IP is responsible for the sending and receiving data packets over the internet.(Address)

Application Layer

- Embraces functions of the OSI session, presentation and application layers.
- The application layer provides the user with the interface to communication.
- The application Layer sends and receives data from transport layer.
- This layer protocol allows a user on one machine to log into a distant machine and work there.
- File transfer protocol provides a way to move data efficiently from one machine to another machine.
- Protocols used in this layer are:
  - HTTP (Hypertext Transfer Protocol)
  - FTP (File Transfer Protocol)
  - Telnet
  - SMPT (Simple Mail Transfer Protocol)

Transport Layer

- Transport Layer is the third layer of the TCP/IP model.
- Transport layer allow peer entities on the source to destination hosts to carry on a conversion.
- Two end to end transport protocols have been defined here.
- Transport Layer Also Handles all error detection & recovery.
- Provides communication session management between host computers.
- TCP provides the reliable connection oriented transport of data between two computers that use Internet Protocol to communicate.
- TCP also handles the flow control.
- UDP is unreliable connection less protocol.
- Protocols used in this layer are:
  - TCP (Transmission Control Protocol)
  - UDP (User Datagram Protocol)

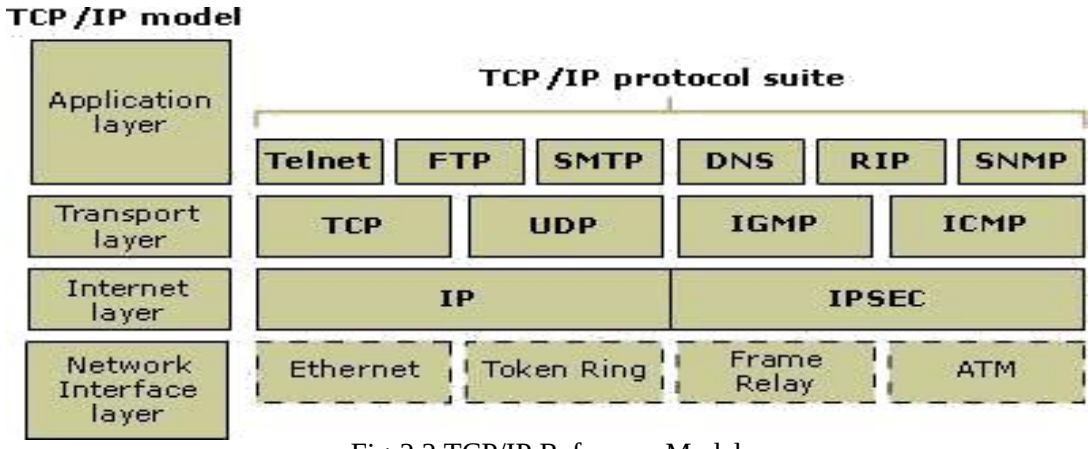


Fig-2.2 TCP/IP Reference Model

Internet Layer

- Internet layer is the second layer of the TCP/IP model.
- The internet layer defines an official packet format and protocol called IP.
- The job of internet layer is to deliver IP packets where they are supposed to go.
- Packages data into IP datagram, which contain source and destination, address information.

- Address is used to forward the datagram between hosts and across networks.
- Protocols Used in this Layer:
  - IP (Internet Protocol)
  - ARP (Address Resolution Protocol)

Network Access Layer

- Specifies details of how data is physically sent through the network.
- Also including how bits are electrically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted-pair copper wire.
- Combination of bottom two layers of OSI model.
- Protocols used in this Layer are :
  - Ethernet
  - FDDI
  - Token Ring

OSI	TCP/IP
OSI = Open system Interconnection	TCP/IP = Transmission Control Protocol / Internet Protocol
It Has 7 Layers	It has 4 Layers
OSI is general Model.	TCP/IP cannot use in any other application.
OSI model have separate Presentation Layer	TCP/IP merge presentation layer with application layer
Protocols are easily replaced as the technology Changes.	Replacing Protocols cannot easy.
Network Layer of OSI model provides both connection oriented and connection less communication	Network layer of TCP/IP provides connection less Connection.

Compression

- Compression is the reduction in size of data in order to save space or transmission time.
- Most often compression is used to minimize storage space (on a hard drive, for example) or for reducing transmitted data over a network.

How Compression work?

- Compression technology uses algorithms to remove extra/repetitive information.
- After compression is applied, the original information is represented by a more compact and efficient format.
- This “compressed” data can then be sent over the network.
- After the compressed data is received at the destination, it is decompressed based on algorithms.
- When you send or receive information on the internet, larger files may be transformed in a ZIP, Gzip, disk archive or other compression format.

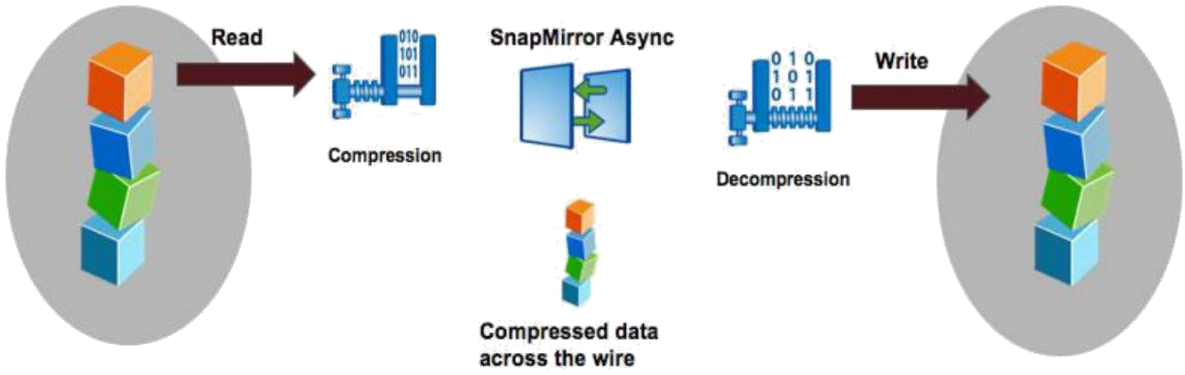


Fig-2.3 Compression

Lossy Compression

- With lossy compression, some loss of information is acceptable.
- The best example is a video conference where there is an acceptable amount of frame loss in order to deliver the image in real time.
- People may grasp for what is happening on the other end of the conference.
- For example, high-resolution details can be lost if a picture is going to be displayed on a low-resolution device.

Lossless Compression

- With lossless compression, data is compressed without any loss of data.
- It assumes you want to get everything back that you put in.
- The process of reducing the size of a data file is referred to as data compression.
- For example: data files
- This kind of compression can reduce a text file to 50% of its original size.

Mapping of network drive

- A network drive is a file folder located on a remote computer that has been configured for sharing over a LAN.
- Mapping a drive simply means to connect a local drive with a specially allocated folder on another computer.
- More than one computer may map their drives to this shared resource.
- It only takes some few steps to map a drive.

Steps to create Map Drive

- Step 1. right-click My Computer
- Step 2. Click Map network drive
- Step 3. In the Drive list, click a drive letter.. You can choose any available letter.
- Step 4. In the Folder box, type the path of the folder, or click Browse to find the folder or computer.

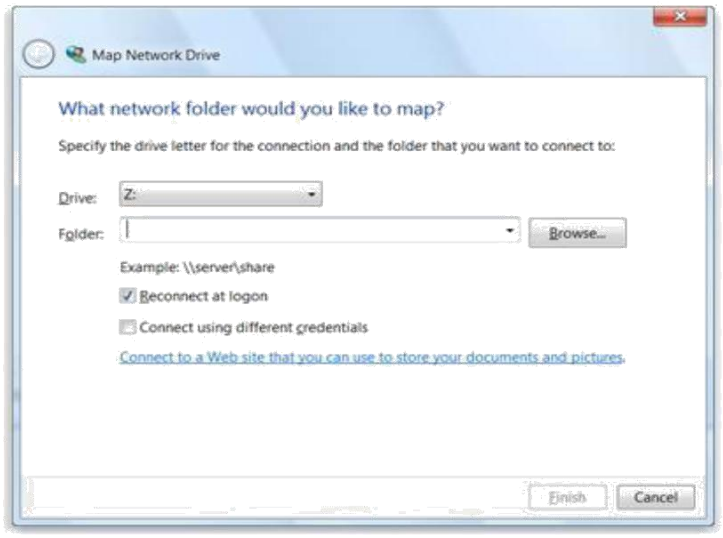


Fig-2.4 Steps to Mapping a drive

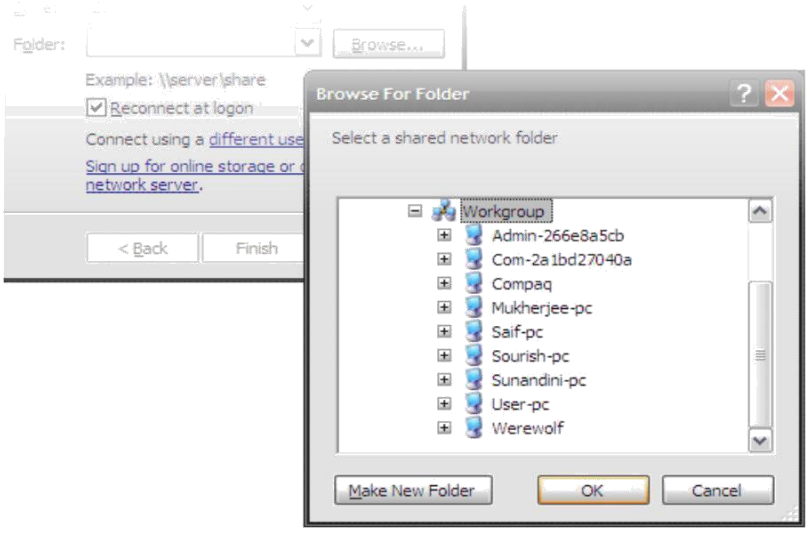


Fig-2.5 Steps to Mapping a drive

- To connect every time you log on to your computer, select the Reconnect at logon check box.
- Step 5. Click Finish.
- To disconnect a mapped network drive, use the tools/disconnect network drive, option right click on my computer and choose disconnect.

❖Disk Quota

- A disk quota is a limit set by a system administrator that restricts certain aspects of file system usage on operating systems.
- The function of using disk quotas is to allocate limited disk space.
- Disk quotas, which allow administrators to control the amount of data that each user can store on an NTFS (Non-Terminal File System), file system volume.
- There are two basic types of disk quotas.
  1) Usages Quota
  2) File Quota
- 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.
- Disk quotas are typically implemented on a per-user or per-group basis.

❖Encryption

- Encryption is the conversion of electronic data into another form, called cipher text, which cannot be easily understood by anyone except authorized parties.
- The translation of data into a secret code.
- Unencrypted data is called plain text*;* encrypted data is referred to as cipher text.
- Following are key elements of security:
  - Authentication: the origin of a message can be verified.
  - Integrity: proof that the contents of a message have not been changed since it was sent.
  - Non-repudiation: the sender of a message cannot deny sending the message.

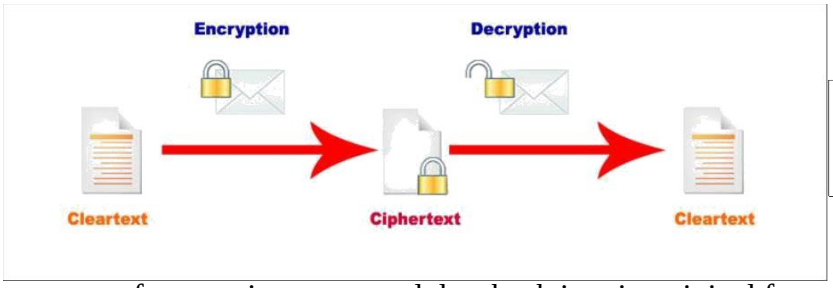


Fig-2.6 Encryption and Decryption

- Decryption is the process of converting encrypted data back into its original form.
- Computer encryption systems generally belong in one of two categories:
  - Symmetric-key encryption
  - Asymmetric encryption / Public-key encryption

Symmetric-key encryption

- Symmetric Encryption is an Encryption algorithm where the same key is used for both Encryption and Decryption.
- The key must be kept secret, and is shared by the message sender and receiver.
- Symmetric-key algorithms can be divided into two,
  - Stream ciphers
  - Block ciphers

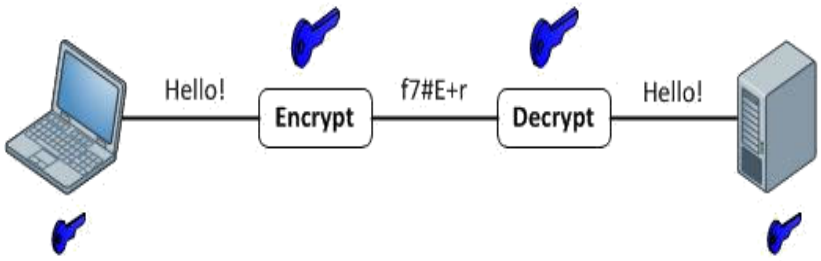


Fig-2.7 Symmetric Encryption

- Stream Cipher
  - Stream ciphers encrypt the bits of the message one at a time
- Block Cipher
  - take a number of bits and encrypt them as a single unit
- Example of Symmetric Key Algorithms,
  - DES (Data Encryption Standards)
  - 3DES
  - AES (Advanced Encryption Standards)

Asymmetric-key Encryption

- It is also known as Public-key Encryption.
- Asymmetric cryptography, requires two pair of separate keys, one is private key an is public key.
- The public key is used to encrypt plaintext or whereas the private key is used to decrypt cipher text.
- The public key is widely distributed, while the private key is known only to its proprietor.
- Example of asymmetric encryption,
  - DSA (Digital Signature Algorithm)
  - RSA (Rivest-Shamir-Adleman)

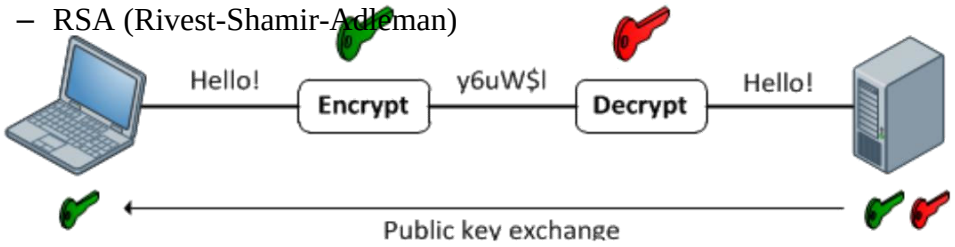


Fig-2.8 Asymmetric Encryption

Net Meeting

- Microsoft introduced the NetMeeting application to allow for VoIP (Voice over Internet Protocol) communications and video conferencing using the internet as the transmission medium.
- NetMeeting delivers a complete Internet conferencing solution for all Windows users with multi-point data conferencing, text chat, and file transfer, as well as point-to-point audio and video.
- It also allowed for application and desktop sharing, remote desktop sharing and transfer of files between client computers.
- NetMeeting was available for use starting with later versions of Internet Explorer 3 and Windows 95 and continued up through Windows XP.
- NetMeeting was one of the most popular applications for video conferencing, until free video conferencing capabilities began to be introduced in applications like Yahoo! Messenger and MSN Messenger.
- Windows Messenger and Microsoft Office Live Meeting for its offering of video conferencing capabilities.

Fig-2.9 Screen view of NetMeeting Application

Full Form:

1) ISO - International Standard Organization
2) OSI - Open System Inter Connection
3) TCP/IP – Transmission Control Protocol / Internet Protocol
4) HTTP - Hypertext Transfer Protocol
5) SMTP - Simple Mail Transfer Protocol
6) FTP - File Transfer Protocol
7) TCP - Transmission Control Protocol
8) UDP - User Datagram Protocol
9) IP - Internet Protocol
10) ARP - Address Resolution Protocol
11) VoIP - Voice over Internet Protocol
12) DES - Data Encryption Standards
13) AES - Advanced Encryption Standards
14) DSA -Digital Signature Algorithm
15) NTFS - Non-Terminal File System

UNIT-2

Transmission Media Multiplexing& Switching Concepts Network Devices

❖ Transmission Media:

- Transmission media is also called Communication channel.
- Transmission media is a physical pathway that carries the information from sender to receiver.
- Transmission media make possible the transmission of electric signals from one computer to another.
- These electric signals express data values in the form of binary, which are the basic for all computer information.
- These signals can be transmitted through copper wires, optical fibers, atmosphere, water and Different Medias have different properties like bandwidth, delay, cost and ease of installation and maintenance.
- Types of Transmission media are,

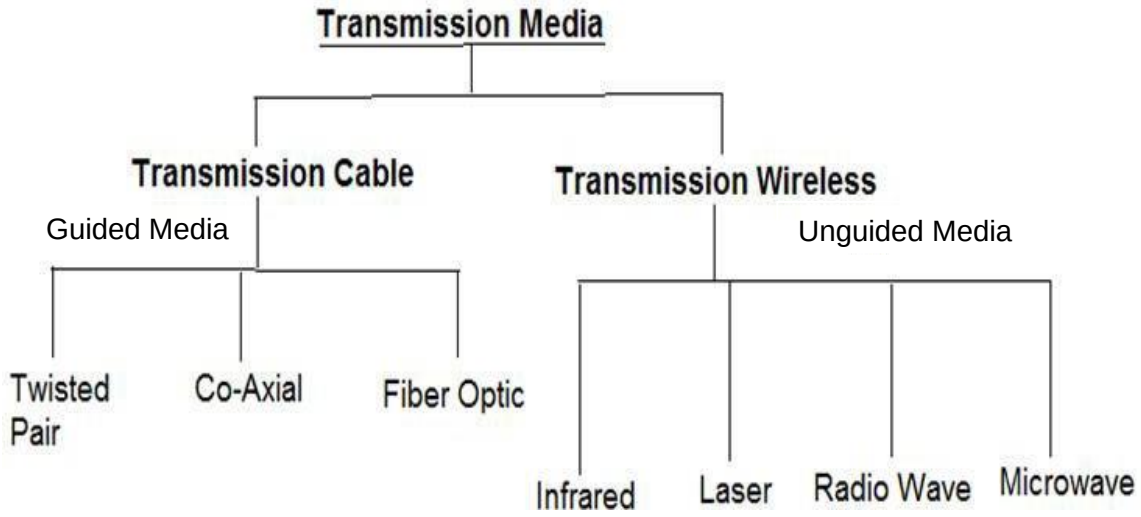


Fig-1 Types of Transmission Media

Guided Media

- Electrical/Optical signals are passed through a solid medium (different types of cables/wires).
- As the path traversed by the signals is guided by the size, shape and length of the wire, this type of media is called guided media.
- Also, in guided media, the signals are confined within the wire and do not outside of the wire/media.
- Guided media divided into following types,
    - Twisted-pair Cable
        - Shielded Twisted Pair (STP)
        - Unshielded Twisted Pair (UTP)
    - Coaxial Cable
        - Thin net Cable
        - Thick net Cable
    - Fiber-optic Cable

Twisted-Pair Cable:

- A cable consisting of two wires twisted round each other called twisted pair.
- Twisted pair is the ordinary copper wire that connects home and many business computers to the telephone company.
- To reduce crosstalk and also protects cable from radio frequency noise.

- Twisted pair comes with each pair uniquely color coded.

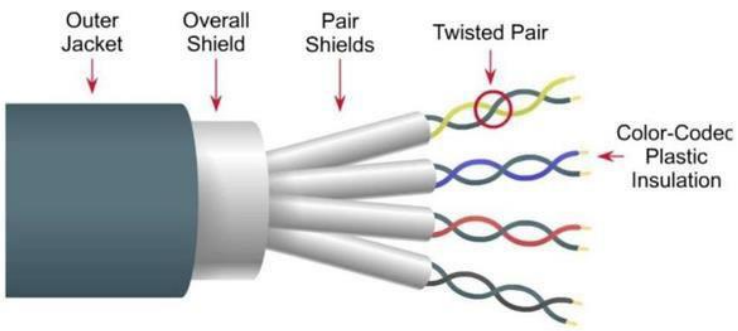


Fig-2 Twisted Pair Cable

- It is a thin, flexible cable that is easy to string between walls.
- More lines can be run through the same wiring.
- There are two types of twisted pair cable,
    - 1) Shielded Twisted Pair (STP)
    - 2) Unshielded Twisted Pair (UTP)

Shielded Twisted Pair:

- Shielded Twisted Pair (STP) Cable.
- STP is similar to UTP but with each pair covered by an additional copper jacket foil wrapping.
- This shielding helps protect the signals on the cables from external interference.
- It includes two pairs of wires within a single shield.
- More Expensive
- STP costs more than coaxial but less costly then thick or fiber optic.
- STP cabling often is used in Ethernet networks, especially fast data rate Ethernets.

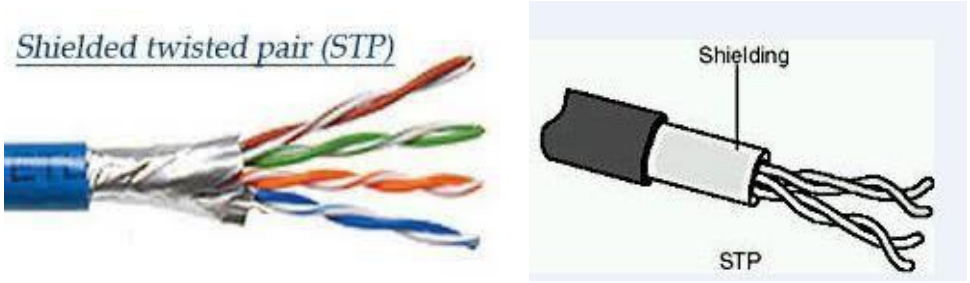


Fig-3 Shielded Twisted-Pair Cable

Unshielded Twisted Pair:

- UTP cable does not incorporate a shielded into its structure.
- Several Twisted pairs can be bundled together in a single cable.
- These pairs are typically color coded to distinguish them.
- Telephone system commonly uses UTP.
- UTP is easy to install.
- UTP cabling does not offer as high bandwidth or as good protection from interference as coaxial or fiber optic cables.

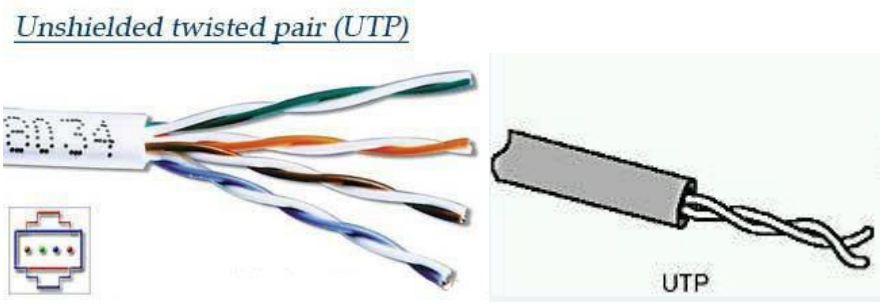


Fig-4 Unshielded Twisted Pair Cable

- Difference between STP and UTP:

  - 'STP' is shielded while 'UTP' is not.
  - STPs are more expensive than UTPs.
  - UTPs are more common in computer shops compared to STPs.
  - STPs are for heavy duty use while UTPs are not.
  - STPs allow maximum bandwidth while UTPs do not.

Fiber optic cable:

- Fiber optic refers to the medium and the technology associated with the transmission of information as light impulses along a glass or plastic wire or fiber.
- A technology that uses glass (fibers) to transmit data.
- A fiber optic cable consists of a bundle of glass threads, each of which is capable of transmitting messages onto light waves.
- Fiber optic cables carry communication signals using pulses of light.

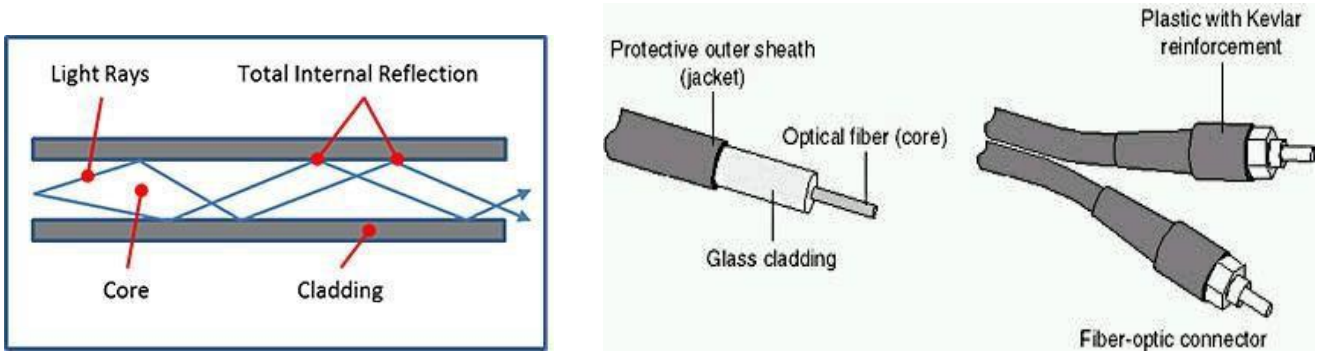


Fig-5 Fiber Optic Cable

- The fiber is coated with a cladding or a gel that reflect signals back into the fiber to reduce signal loss.
- **Core** - Thin glass center of the fiber where the light travels
- **Cladding** - Outer optical material surrounding the core that reflects the light back into the core
- **Coating** - Plastic coating that protects the fiber from damage.
- In order for optical fibers to transmit data over long distances, they need to be highly reflective.
- Fiber optic cable comes into two types,
  - Single mode fiber
  - Multi-mode fiber
- Fiber optic cables have a much greater bandwidth than other cables.
- Fiber optic cables are much thinner and lighter than metal wires.
- Fiber optic cable is used to transmit the long distance data transmission.
- Medical: Used as light guides, imaging tools and also as lasers for surgeries.

- as wiring in aircraft, submarines and other vehicles
- The Main Disadvantages of fiber optic the glass fiber requires more protection within an outer cable than copper. For these reasons and because the installation of any new wiring is expensive.

Coaxial Cable:

- Coaxial cable was invented in 1880.
- AT&T established its first coaxial transmission system in 1940.
- The coaxial cable is a copper-based wire cable. It is composed of four separate layers.
- The center of the cable has a thin wire conductor. Surrounding the copper wire is a layer of plastic insulation.
- Coaxial cables are inexpensive.
- Components of Coaxial Cables are,
- **Center Conductor -**It is made of solid copper wire.
- **An Outer Conductor -** This outer Conductor is also called "Shielded", serves as ground and also protects the center conductor from EMI (Electromagnetic Interface).

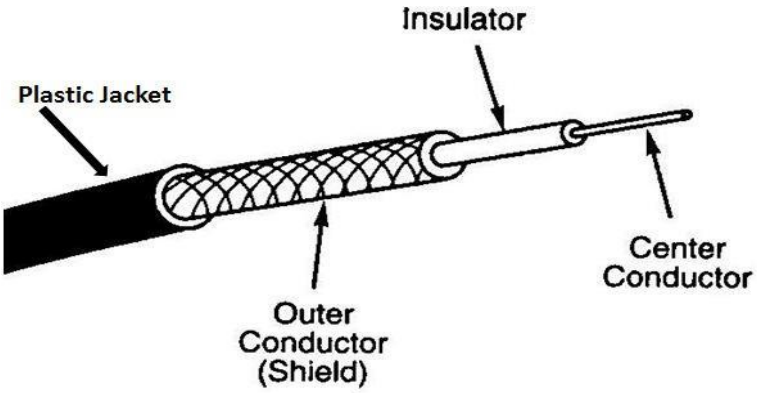


Fig-6 Coaxial Cable

- **An insulation layer -** It is between center conductor and outer conductor.
- **Plastic jacket -** It protects cable from any damage.
- Coaxial Application
  - Television Distribution
  - Long Distance Telephone Transmission
  - Short Distance computer system link
  - Local Area Network

Thin net cable:

- Thin net cable is a light flexible and less expensive cable medium.
- It is easy to install.
- Thin net is about 0.25 inches (6 mm) thick.
- Thin net cable signal transmit for about 185meters (610 feet).

Thick net cable:

- Thick net cable is thicker then thin net.
- Thick net is approximately 0.5 inches (13mm) diameter.
- It does not bend easily.

- It can carry more signals at longer distance.
- It can transmit a signal about 500 meters.(1650 feet)
- It is more expensive then thin net.

Compression of Different Cables				
Cable Type	**Cost**	**Installation**	**Capacity**	**Range**
Coaxial Cable Thin net	Less than STP	Inexpensive/easy	10 Mbps	185 m
Coaxial Thick net	Greater than STP and less than fiber optic	Easy	10 Mbps	500 m
Shielded Twisted Pair (STP)	Greater than UTP and less than thick net coaxial	Fairly Easy	16 Mbps up to 500 Mbps	100 m
Unshielded Twisted Pair (UTP)	Lowest	Inexpensive/easy	10 Mbps up to 100 Mbps	100 m
Fiber Optic cable	Highest	Expensive/ Difficult	100 Mbps	10s of Kilometer

Unguided Media:

- Unguided media relates to data transmission through the air by antenna; is commonly referred to as wireless.
- It called unguided or wireless because there is nothing to guide them analog a specific path, like in wires.
- Wireless communication is used where cables are difficult to use or install.
- Reasons for Wireless Technology:
    - Spaces where cabling would be impossible
    - People who travel outside of the network environment and need instance access to network resources.
- Classification of Wireless Transmission:
    - Directional
        - Satellite communication systems
    - Omni direction
        - mobile communication systems
- Types of unguided media are,
    - Infrared
    - Radio
    - Bluetooth
    - Microwave
    - Laser

Infrared

- Infrared is a wireless transmission medium that carries data via light beams.
- Transmission and receiver must be in straight line.
- Transmission must occur over a clear line of sight path between transmission and receiver.
- Infrared transmissions are typically limited within 100 feet.
- Infrared high band width support transmission speed of up to 10 mbps.
- Four various infrared communications are as follow,

- **Broadband optical point**:
  - This method uses broadband technology. Data transfer rates in this high-end option are competitively with those for a cable based network.
- **Line-of-sight infrared**:
  - Transmission must occur over a clear line-of-sight path between transmitter and receiver.
- **Reflective Infrared**:
  - Wireless PCs transmit toward a common, central unit, which then directs communication to each of the nodes.
- **Scatter Infrared:**
  - Transmission reflects off floors, walls and callings until they finally reach the receiver. Data transfer rate is slow. The maximum reliable distance is around 100 feet.

- Applications uses infrared are,
  - Car locking systems
  - Mouse
  - Home security systems
  - TVs, VCRs, CD players, stereos remotes
  - Toys
- Advantages:
  - Low power requirements
  - High noise immunity
  - Low costs
- Disadvantages:
  - Line of sight
  - Short range
  - Blocked by common materials: people, walls can block transmission

Laser Transmission

- Laser is a powerful source of light having extraordinary properties which are not found in the normal light.
- The unique property of laser is that its light waves travel very long distances
- High powered laser transmission can transmit data for several thousand yards when line of sight communication is possible.
- Laser light technology is similar to infrared technology.
- Laser light technology is employed in both LAN & WAN transmissions, through it is more commonly used in WAN transmission.

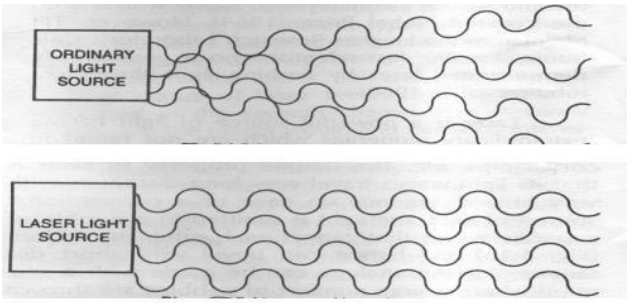


Fig-7 Laser Transmission

- Application are used laser technology are,
  - Laser Printer
  - High speed photography
  - information encoded into the surface of the CD

Radio

- Radio is the wireless transmission of electromagnetic signals through the atmosphere or free space, information such as sound.
- A network that uses electromagnetic radio waves operates at radio frequency and its transmission is called RF transmission.
- Each host on the network attached to an antenna, which can both send and receive RF.
- Radio Transmission does not required line of sight.
- A machine that sends radio signals is called a transmitter, while a machine that "picks up" or receive the signals is called a receiver.
- A machine that does both jobs is called a "transceiver".
- When radio signals are sent out to many receivers at the same time, it is called a broadcast.
- Frequency: Frequency describes the number of waves that pass a fixed place in a given amount of time.
- Radio signals can be ling range (Cities) and short range (Within a building).
- Radio waves are used for multicast communication, such as Television and radio.
- Radio signals can use Omni directional antennas.
- Radio signals used different frequency range 3 kHz to 300 kHz.
- Use of Radio Transmission,
    - Audio
    - Telephony
    - Video
    - Digital Radio
- Advantages,
    - Cheap
    - No license needed
    - High speed
    - Covers large area
- Disadvantages,
    - Greater power consumption
    - Limited frequency

Microwaves

- Microwave transmission is usually point-to-point using directional antennae with a clear path between transmitter and receiver.
- Microwaves are high frequency radio frequency.
- Microwaves are used for unicast communications.
- The distance covered by microwave signals is based upon the height of the antenna.
- In order to increase this coverage each antenna has a built-in repeater that regenerates the signal before passing it on to the next antenna in line.
- Microwave equipment can be used to transmit both analog and digital microwave signals.
- Microwave data is sent from site to site sequentially, and can be sent from either side.
- This is known as “backhauling”.
- Microwaves uses in cellular telephones, satellite networks and wireless LANs.
- Microwave transmission relies on three key elements:
    - Use of radio frequency to achieve the transmissions (operating between 1Ghz to 170Ghz)
    - Clear line-of-sight with no obstacles in the way.
    - Regular relay stations required due to line of site and cost considerations.

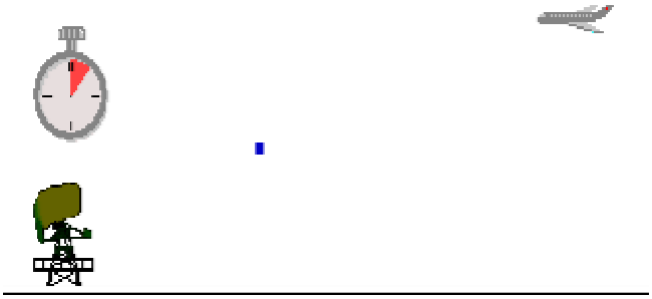


Fig-8 Use of Microwave Signals

- Advantages:
  - No cables needed
  - Multiple channels available
  - Wide bandwidth
- Disadvantages:
  - Line-of-sight will be disrupted if any obstacle, such as new buildings, are in the way
  - Signal absorption by the atmosphere like rain
  - Towers are expensive to build

Bluetooth

- A standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.
- Bluetooth is a wireless technology standard for exchanging data over short distances.
- The name Bluetooth is borrowed from Herald Bluetooth, a king in Denmark more than 1,000 years ago.
- Bluetooth was standardized as IEEE 802.15.1, for the low power radio communications to link phones, computers and other network devices over short distance without wires.
- A master Bluetooth device can communicate with a maximum of seven devices.
- Data can be transferred between the master and one other device, the master chooses which device to address.
- When two Bluetooth enabled devices connect to each other, this is called pairing.
- Signals transmitted with Bluetooth in very short range, a minimum range of 10 meters or 30 feet.
- Data can be exchanged at a rate of 1 mbps per second.
- The key features of Bluetooth technology are low power, and low cost.

- Advantages:
  - Bluetooth does not require a clear line of sight between the devices.
  - The processing power and battery power that it requires in order to operate is very low.
  - One major advantage is its simplicity of use. Anyone can figure out how to set up a connection and sync two devices with ease.
  - the technology is completely free of charge

- Disadvantages:
  - It only allows short range communication between devices.
  - It can only connect two devices at once.
  - If installed on a cell phone it is free to receiving cell phone virus.
  - When using Bluetooth internet, the connection can sometimes run very slow.
  - Data sent between two Bluetooth devices has a maximum transfer speed of 1 mbps per second. Other technology like Infrared and Wi-Fi capable of transferring data at even higher.

Guided Media	Unguided Media
The signal energy propagates within the guided media. i.e. wires	The Signal energy propagates through air.
It is mainly suited for point-to-point communication.	It is mainly used for broadcasting purpose.
The signals propagate in the form of voltage, current and photons.	The signals propagate in the form of electromagnetic waves.
Example of guided media are, Twisted-Pair Cable Coaxial Cable Fiber optic Cable	Example of unguided media are, Infrared Bluetooth Microwaves

❖ Difference Frequency Ranges:

- **Frequency: Frequency describes the number of waves that pass a fixed place in a given amount of time.**

- Each frequency range has a band designer and each range of frequencies behaves differently and performs different frequency.
- The Frequency spectrum is shared by civil government, and military users of all nations according to International Telecommunications Union (ITU).

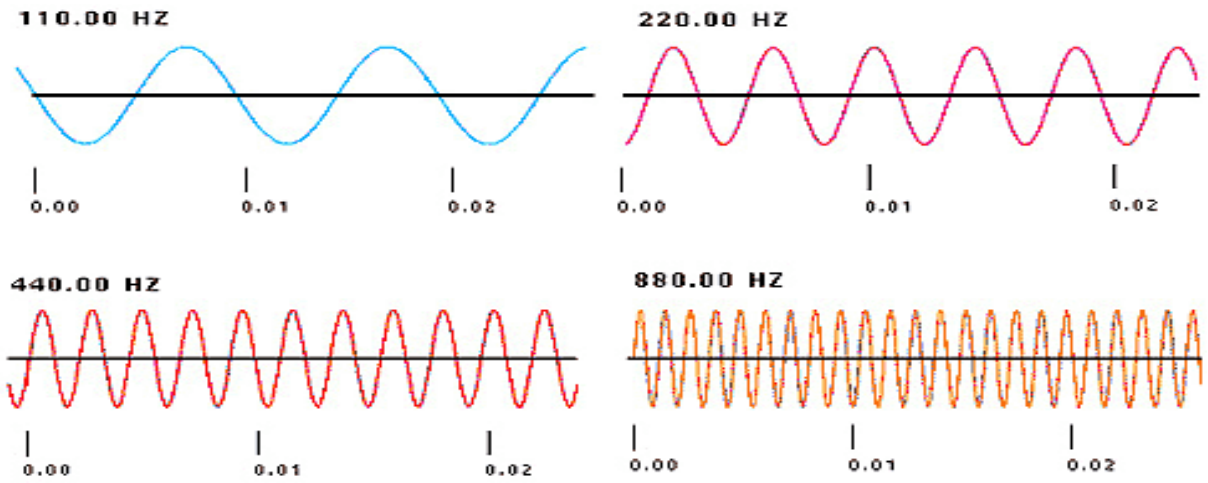


Fig-1 Difference Frequency

- Frequency Standards is describes in International Telecommunications Union radio regulations. And it looks as Follow,

Band	Propagation	Range	Application
Very low frequency (VLF)	Ground	3-30 kHz	Long range radio navigation
Low frequency (LF)	Ground	30-300 kHz	Navigation locators
Middle frequency (MF)	Sky	300 kHz-3 MHz	AM radio
High frequency (HF)	Sky	3-30 MHz	Citizen band (CB) ship/aircraft communication
Very high frequency (VHF)	Sky and line of sight	30-300 MHz	VHF TV,FM radio
Ultrahigh frequency (UHF)	Line of sight	300 MHz-3 GHz	UHF TV, paging, cellular phones, satellite
Super high frequency (SHF)	Line of sight	3-30 GHz	Satellite communication
Extremely high frequency (EHF)	Line of sight	30-300 GHz	Satellite, radar

Fig-2 Table of Difference Frequency Range

❖ Multiplexing & DE multiplexing:

- Multiplexing - To combine multiple signals for transmission over a single line or media.
- Multiplexing is independent signals may be simultaneously transmitted to network.
- Multiplexing is the technique performed in the physical layer of OSI model.
- Aim of multiplexing is,
  - To maximize the utilization of channel.
  - To share an expensive resource.
- Phone calls are a good example of multiplexing in telecommunications. That is, more than one phone call is transmitted over a single medium.

Multiplexing is done by using a device called multiplexer (MUX) that combines n input lines to generate one output line i.e. (many to one)

- Multiplexer (MUX) has several inputs and one output.

At the receiving end, a device called De-multiplexer (DEMUX) is used that separates signal into its component signals. (one to many)

- So DEMUX has one input and several outputs.

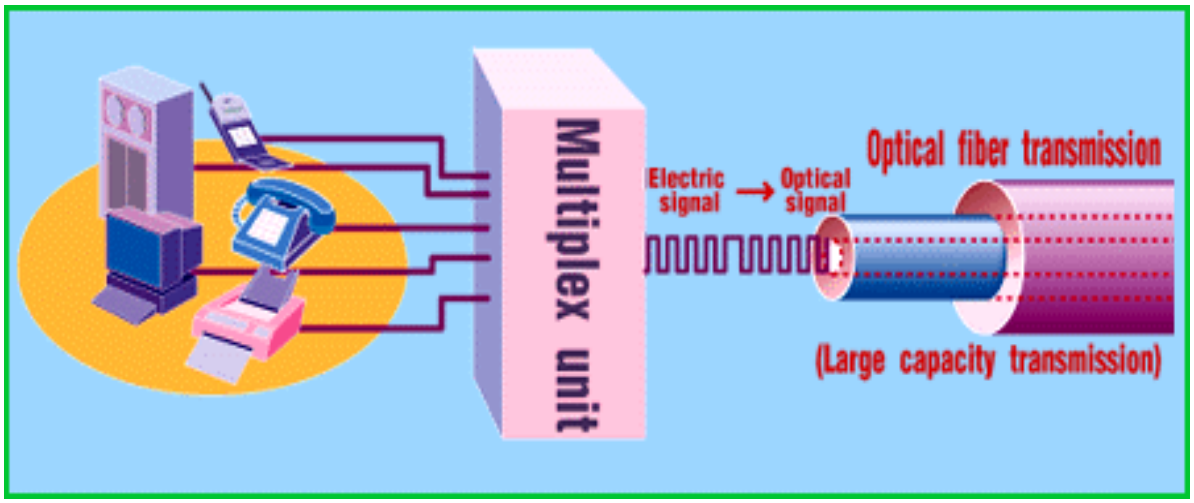


Fig-3 Concept of Multiplexing

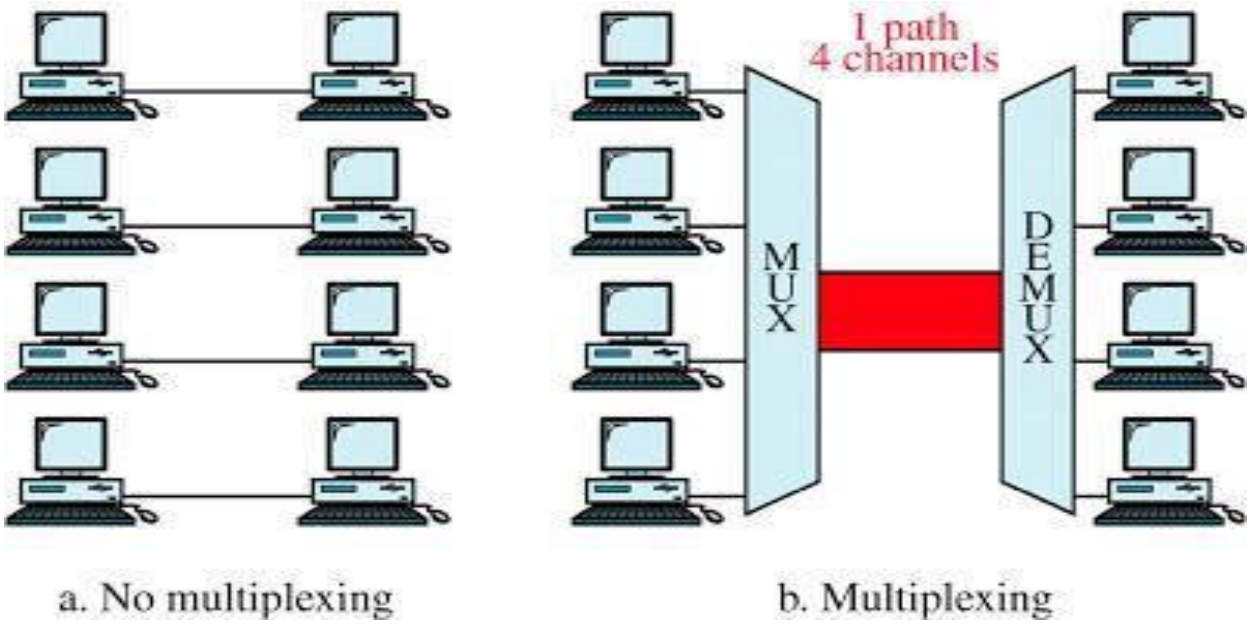


Fig-4 Multiplexing and DE multiplexing

- As shown in Figure-6, Multiplexer takes 4 input lines and diverts them to single output line.
- The signal from 4 different devices is combined and carried by this single line.
- At the receiving side, a de-multiplexer takes this signal from a single line & breaks it into the original signals and passes them to the 4 different receivers.

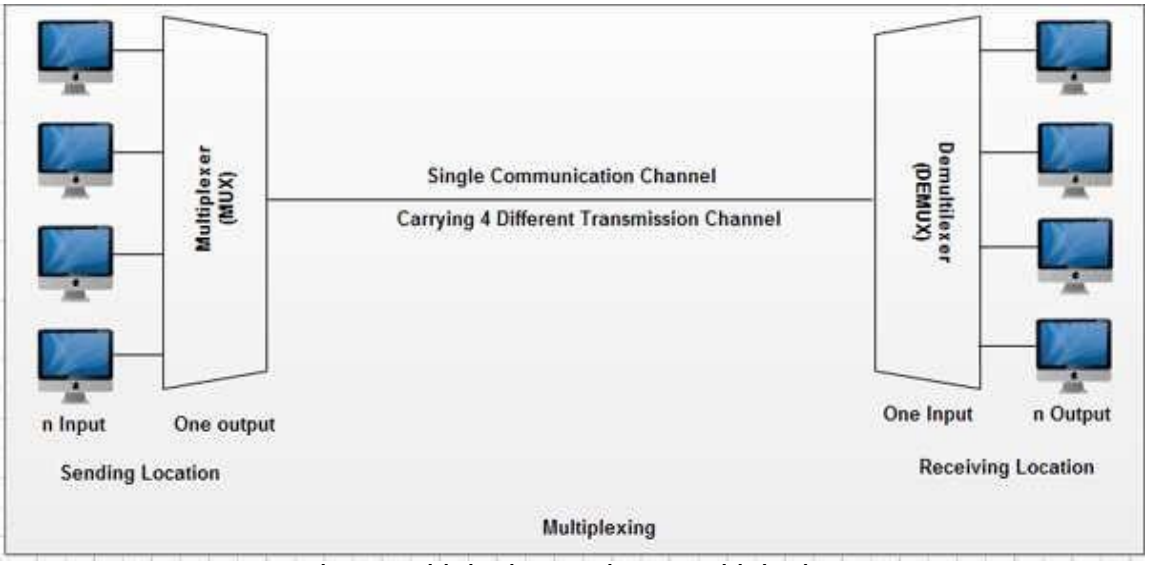


Fig-5 Multiplexing and DE multiplexing

- Multiplexing Applications:
  - Telephone System
  - Satellites
  - Broadcasting (radio and TV)
  - Telemetry

- Advantages of multiplexing:
  - It reduces number of wires.
  - It reduces circuit complexity and cost.
  - It simplifies logic design.

- Disadvantages of multiplexing:
  - The main disadvantage of multiplexes is that they are too expensive.

- Multiplexing Technique divide into several types such as,

  - Analog Multiplexing

    - FDM (Frequency Division Multiplexing)
    - WDM (Wave Division Multiplexing)

  - Digital Multiplexing

    - TDM (Time Division Multiplexing)
      - Synchronous TDM
      - Asynchronous TDM

    - CDM (Code Division Multiplexing)

- **Frequency Division Multiplexing:**

- Frequency Division Multiplexing (FDM) is a networking technique in which multiple data signals are combined for transmission on a single communications line or channel.
- When FDM is used to allow multiple users to share a single physical communications medium the technology is called frequency-division multiple access (FDMA).
- Each signal is assigned a different frequency within the main channel.
- **FDM is a scheme in which numerous signals are combined for transmission on a single communication line or channel. Each signal assigned a different frequency within the main channel.**
- In FDM signal generated by each sending device in different carrier frequencies.
- These signals are then combined in to a single composite signal that can be transmitted by the link.
- FDM is an analog multiplexing technique that combines signal.
- In FDM, signals to be transmitted must be analog signals. Thus digital signals need to be converted to analog form, if they are to use FDM.
- Example: Radio, television broad casting, etc.

- Advantages OF FDM,
    - Simple
    - Inexpensive
    - Popular with Radio, TV, Cable TV
    - All the receivers, cellular telephones, need not to be at the same location
    - A large number of signals can be transmitted simultaneously.

- Disadvantages OF FDM,
    - In Frequency division multiplexing system, a problem for one user can sometime affect others.
    - If the frequencies of two channels are too close, interface can occur.
    - Designers choosing a set of carrier frequencies with a gap between them known as a guard band.
    - Analog signal only having limited frequency range.

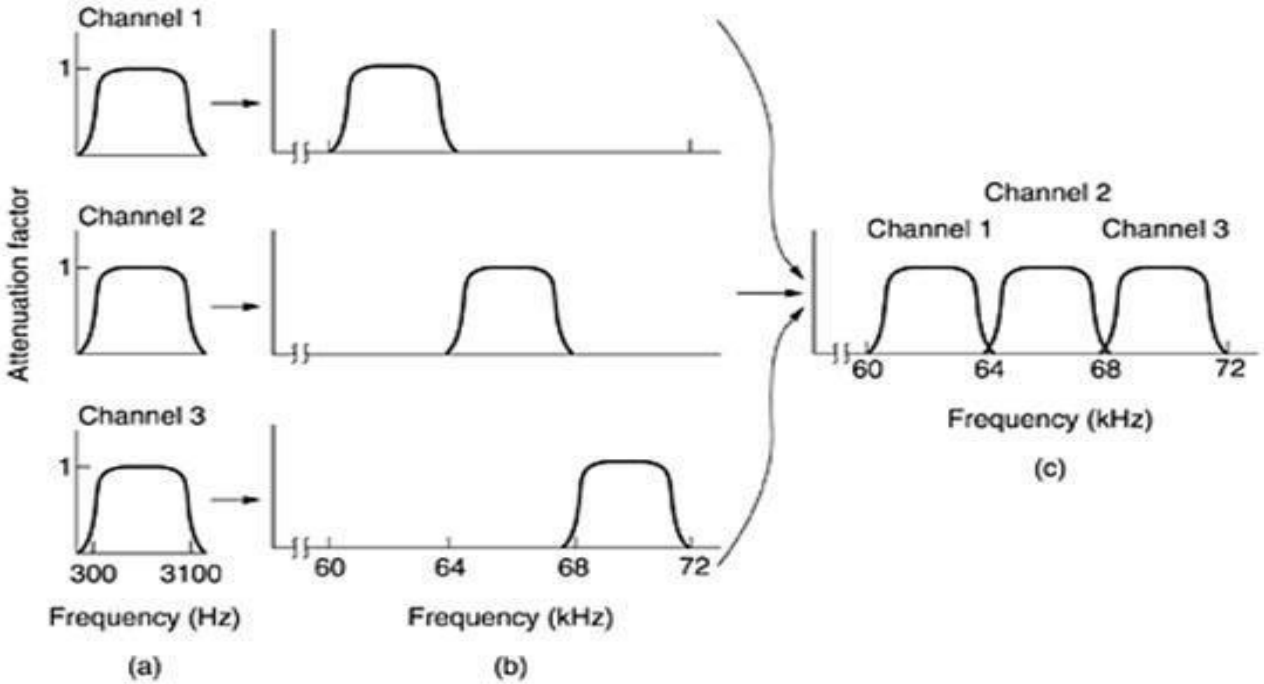


Fig-6 Frequency Division Multiplexing

- **Time Division Multiplexing:**

- Time division multiplexing (TDM) is also known as a digital circuit switched.
- TDM is the digital multiplexing technique.
- **TDM is a method of putting multiple data stream in a single signal by separating the signal into many segments, each having a very short duration.**
- Each individual segment is reassembled at the receiving end based on the timing.
- In TDM, the link is not divided on the basis of frequency but on the basis of time.
- Each user is allotted a particular a short time interval called time slot or time slice during which the data is transmitted by that user.
- In TDM all the signals are transmitted one-by-one.
- Thus each signal will be transmitted for a very short time.
- One cycle or frame is said to be complete when all the signals are transmitted once on the transmission channel.
- Types of TDM,
    - 1. Synchronous TDM
    - 2. Asynchronous TDM

- **Synchronous TDM**

    - It is widely used throughout the Internet.
    - **In synchronous TDM, each device is given same time slot to transmit the data over the link, the fact that the device has any data to transmit or not.**
    - The multiplexer allocates exactly the same time slot to each device at all times, whether or not device has anything to transmit.
    - Each device places its data onto the link when its time slot arrives i.e. each device is given the line turn by turn.
    - If any device does not have data to send then its time slot remains empty.
    - The various time slots are organized into frames.
    - If there are n sending devices, there will be n slots in frame i.e. one slot for each device.

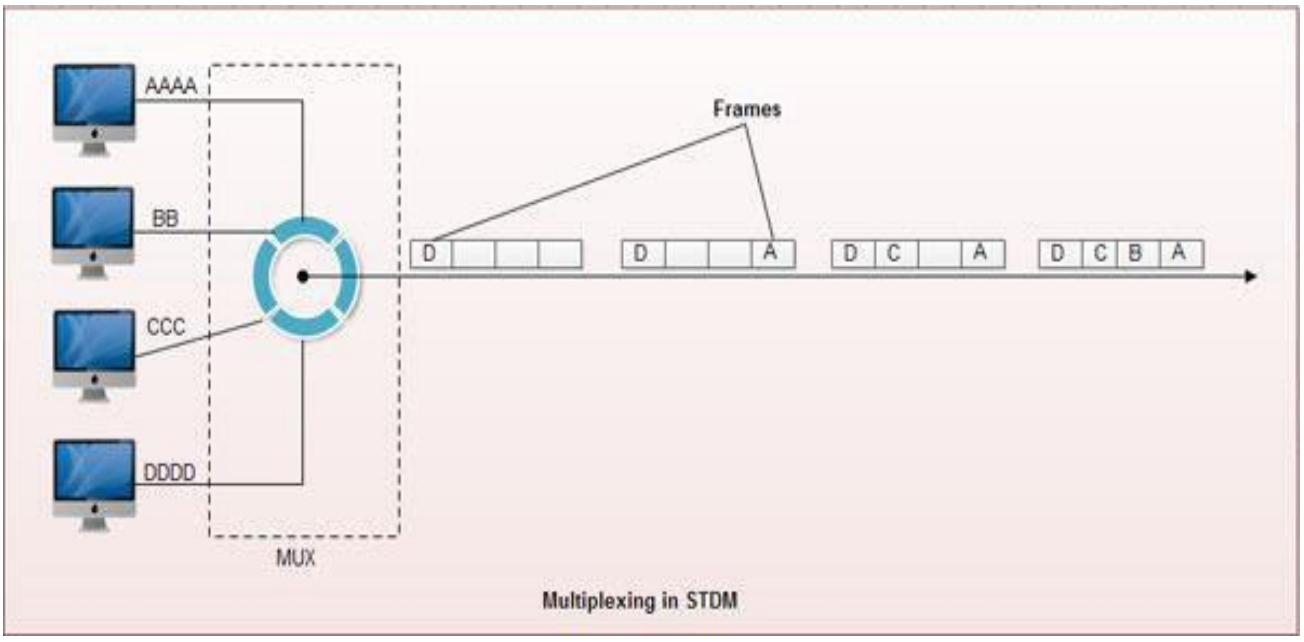


Fig-7 Synchronous Time Division Multiplexing

- **Asynchronous TDM**

  - Each slot in frame is not dedicated to the fix device.
  - **Asynchronous TDM is called so because is this type of multiplexing, time slots are not fixed i.e. the slots are flexible.**
  - The number of slots in a frame is not necessary to equal to be the number of input devices.
  - More than one slot in frame can be allocated for an input device.
  - Suppose number of inputs =4, then number of slots in each frame = 3.
  - Asynchronous Multiplexer transmits only the data from active work stations.
  - If the workstation is not active, no space is wasted on the multiplexed streams.

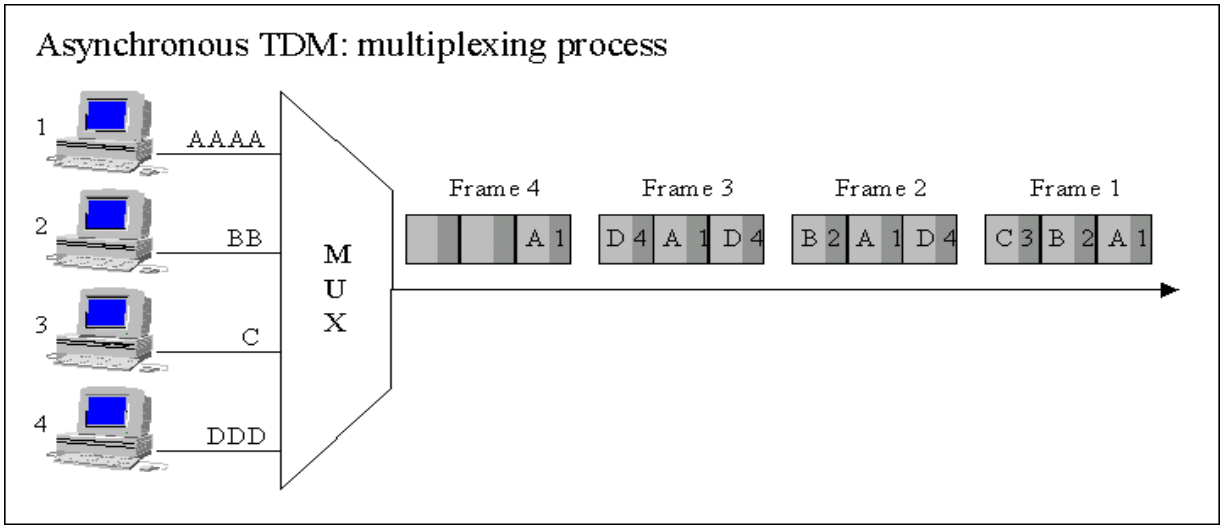


Fig-8 Asynchronous Time Division Multiplexing

- **Wave Division Multiplexing (WDA)**

Wavelength-division multiplexing (WDM) is a technology which multiplexes a number of optical signals onto a single optical fiber by using different wavelengths (i.e., colors) of laser light.

- The term wavelength-division multiplexing is commonly applied to optical signals.
- A WDM system uses a multiplexer at the transmitter to join the signals together and a de-multiplexer at the receiver to split them apart.
- WDM is similar to FDM, but instead of taking place at radio frequencies (RF), WDM is done in the IR portion of the electromagnetic spectrum.
- The use of WDM can multiply the effective bandwidth of a fiber optic communications system by a large factor, but its cost must be weighed against the alternative of using multiple fibers bundled in to cable.

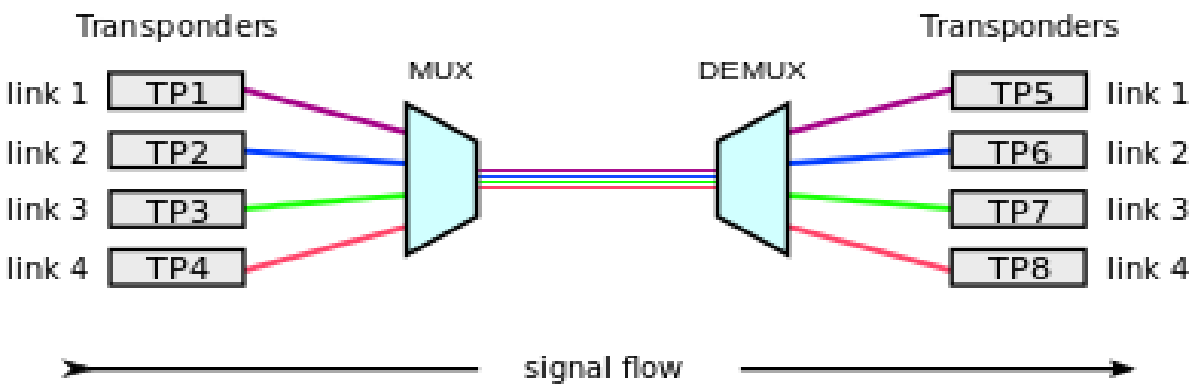


Fig-9 Wave Division Multiplexing

- **Code Division Multiplexing**

- CDM also called spread spectrum technology.
- **Code division multiplexing (CDM) is a networking technique in which multiple data signals are combined for simultaneous transmission over a common (same) frequency band.**
- CDM refers to any of several protocols used in so called second-generation (2G) and third-generation (3G) wireless communications.
- When CDM is used to allow multiple users to share a single communications channel, the technology is called code division multiple access (CDMA).
- CDMA employs analog-to-digital conversion (ADC) in combination with spectrum technology.
- CDM is widely used in second-generation (2G) and third-generation 3G wireless communications.
- The technology is used in ultra-high-frequency (UHF) cellular telephone systems.

❖ Switching

- A switched network is made up of a series of interconnected nodes called switches.
- **Switching Techniques - In large networks there might be multiple paths linking sender and receiver.**

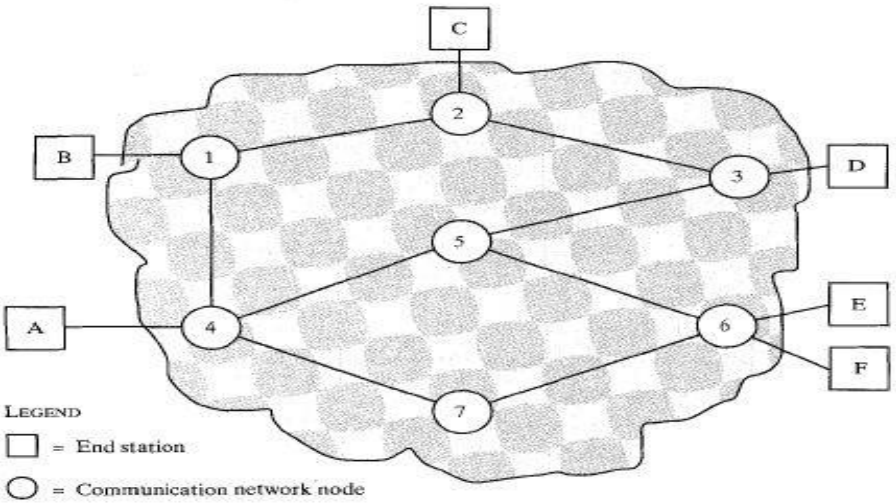


FIGURE 8.1 Simple switching network.

Fig-11 Switching Technique

- In a large network there might be multiple paths linking sender and receiver. Information may be switched as it travels through various communication channels.
- There are basically three types of switching methods are made available.
- Out of three methods, circuit switching and packet switching are commonly used.

1) Circuit Switching

2) Packet Switching

3) Message Switching

- **Circuit Switching**

- A type of communications in which a dedicated channel (or circuit) is established for the duration of a transmission.
- **Circuit-switched is a type of network in which a physical path is obtained for and dedicated to a single connection between two end-points in the network for the duration of the connection.**
- With this type of switching once a connection is established, a dedicated path exists between both ends until the connection is terminated.
- A complete end-to-to path must exists before communication can take place.
- Circuit-switching networks are sometimes called connection-oriented networks.
- Ordinary voice phone service is circuit-switched.
- The telephone company reserves a specific physical path to the number you are calling for the duration of your call.
- During that time, no one else can use the physical lines involved.
- Advantage is that it provides for non-stop transfer without requiring packets and without the traffic usually needed, making maximal and optimal use of available bandwidth for that communication.

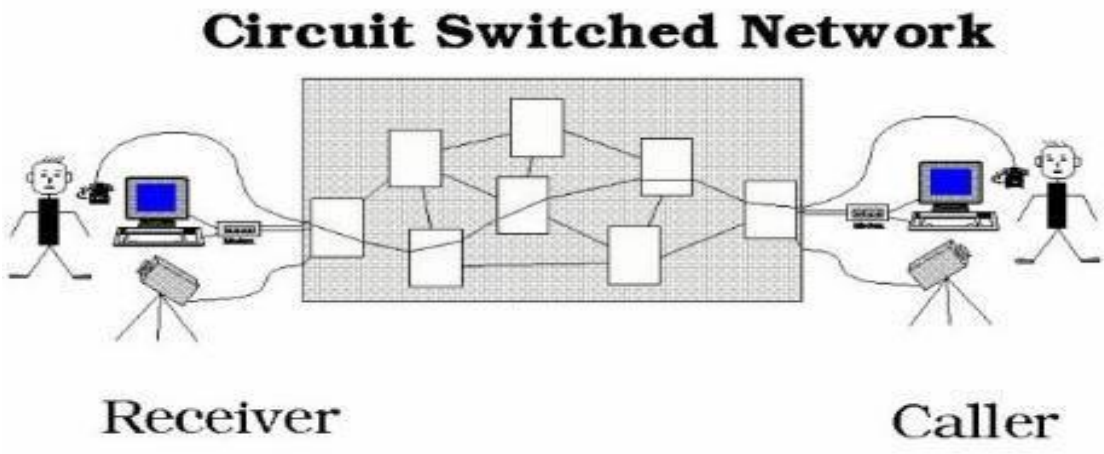


Fig-12 Circuit Switching Technique

- Advantages:
    - Guaranteed bandwidth
    - Simple abstraction
        - Reliable communication channel between hosts
        - No worries about lost or out-of-order data
    - Simple forwarding
        - Forwarding based on time slot or frequency
- Disadvantages:
    - Wasted bandwidth
        - traffic leads to idle connection during silent period
    - Blocked connections
        - Connection refused when resources are not sufficient
    - Connection set-up delay
        - No communication until the connection is set up
    - Network state
        - Network nodes must store per-connection information

- **Packet Switching**

- **Packet switching is a digital networking communications method that groups all transmitted data – regardless of content, type, or structure – into suitably-sized blocks, called packets**.
- **Packets are transfer via different network devices/routs for fast and efficient transmission.**
- When a computer attempts to send a file to another computer, the file is broken into packets.
- These packets are then routed by network devices to the destination.

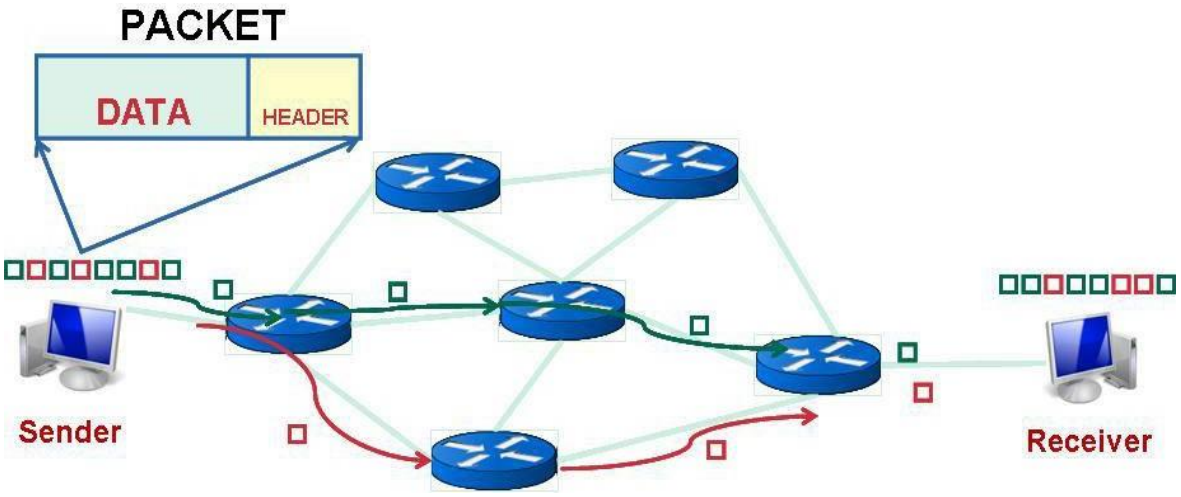


Fig-13 Packet Switching Method

- Advantages:
    - Packet switching is cost effective.
    - Packet can be rerouted if there is any problem, such as busy or disabled link.
    - Many network users can share the same channel at the same time.

- Disadvantages:
    - Protocols for packet switching are more complex.
    - If packet is lost, sender needs to retransmit the data.

- There are two major modes of packet switching:
    - Connectionless Packet Switching
    - Connection oriented Packet Switching

- **Connection less Packet Switching**

    - Each packet contains complete addressing or routing information and is routed individually.
    - This can result in out-of-order delivery and different paths of transmission.
    - This technique is also known as datagram switching.

- **Connection Oriented Switching**

    - Data packets are sent sequentially over a predefined route.
    - Packets are assembled, given a sequence number and then transported over the network to a destination in order.
    - In this mode, address information is not required.
    - Also known as virtual circuit switching.

- **Message Switching**

With message switching there is no need to establish a dedicated path between two stations.

- When message sends a message, the destination address is appended to the message.
- In message switching, the source and destination nodes are not directly connected.
- Instead, the intermediary nodes (mainly switches) are responsible for transferring the message from one node to the next.
- Thus, every intermediary node inside the network needs to store every message prior to retransferring the messages one-by-one as resources become available.
- If the resources are not available, the messages are stored indefinitely. This characteristic is known as store and forward.
- Because message switching implements the store-and-forward technique, it efficiently uses the network.
- Also, there is no size limit for the messages.
- Email is a common application for message switching.

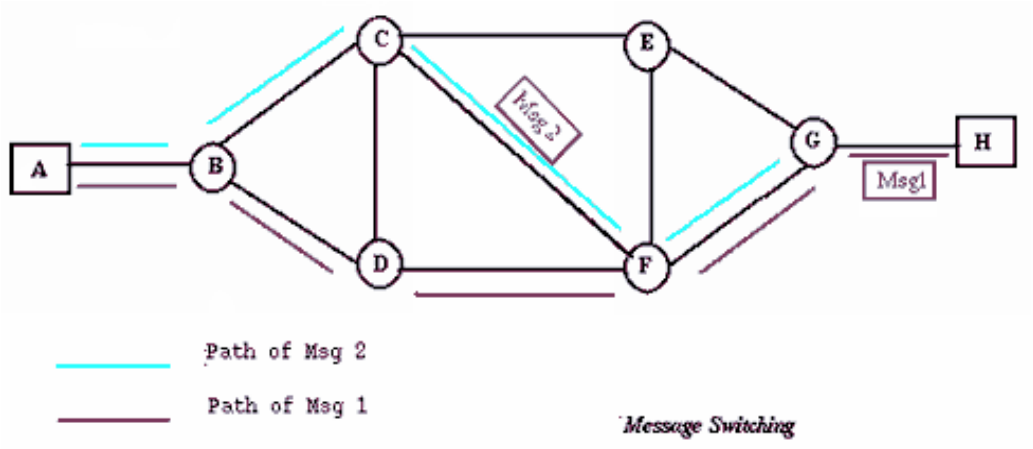


Fig-14 Message Switching Method

- Advantages:
    - Data channels are shared among communication devices.
    - Messages can be stored temporarily at message switches.
    - Priorities may be used to manage network traffic.
    - Message broadcasting can be achieved with the use of broadcast address appended in the message.

- Disadvantages:
    - Store and forward devices are expensive, because they must have large disks to hold potentially ling message.
    - Message-switched networks are very slow as the processing takes place in each and every node, which may result in poor performance.
    - This technique is not adequate for interactive and real-time processes, such as multimedia games and voice communication.

- Difference between circuit switching and packet switching

Circuit Switching	Packet Switching
Circuit switching is done at physical layer	Packet switching is generally done at network layer.
Circuit switching requires the resources to be reserved before the transmission of data	Packet switching doesn't require such reservation of resources.
In circuit switching, whole of the data travels along a single dedicated path.	Packet switching data is divided into packets and each packet are treated independently and travel along different paths.

Network Devices

- Computer networking devices are units that mediate data in a computer network.
- Computer networking devices are also called network equipment, Intermediate Systems (IS) or Inter Working Unit (IWU).

Layer 1 Devices

- Physical Layer Devices are,
- LAN card
- Modem
- DSL (Digital Subscriber Line/Loop) & ADSL (Advanced/Asymmetric Digital Subscriber Line)
- Hub
  - Active
  - Passive
  - Smart
- Repeater

❖ LAN Card or NIC (Network Interface Controller)

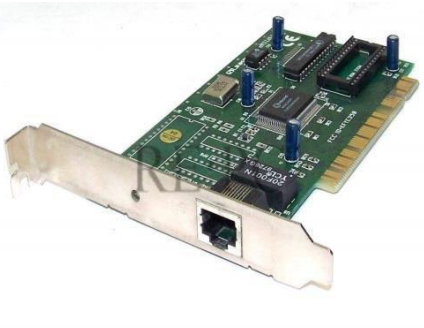
- The LAN (Local Area Network) card is a 'door' to the network from a computer.
- Any type of network activity requires a LAN card: the Internet, network printer, connecting computers together, and so on.
- Today many devices contain a network card, including televisions for their Internet apps, mobile phones, VoIP, desk phones, and even refrigerators.
- LAN cards are hardware devices that can be added to a computer, or they can be integrated into the main hardware of the computer.
- A Local area network card or LAN Card is a small piece of hardware, which is connected inside a PC to link a computer network.
- NIC provide a dedicated, full-time connection to a network.

- LAN Card Types,
  - There are many other ways of connecting the LAN card to a computer.
  - Some cards are connected via the USB (universal serial bus) port, some via the PCI (Peripheral Component Interface) port inside of the computer, and some are even embedded inside of the computer.
  - Most laptops today have integrated LAN cards both for wired and wireless networking.
  - A PCI card goes inside of a PC computer.
  - The card shows an Ethernet port, which is the spot where you plug in a network cable.

- The LAN card you select often determines the protocols that are used on the network.
  - For example, an Ethernet card will allow communication via the Ethernet protocol.
  - A co-axial card would allow for a bus topology network.
  - A fiber cable would have a different cable plug-in, and it would likely work with Wide Area Network protocols.

Prepared By: Thummar P. V.

a. Fiber Optic Port



b. PCI Port

c. USB Port

- Function of LAN card
  - The purpose of a LAN card is to create a physical connection to the network.
  - The first interface supported by a LAN card is a physical interface through which the cable plugs into the card.
  - The second function of a LAN card is to provide a data link.
  - The first two layers are the physical layer and the data link.
  - Each layer of the OSI model allows for other layers to be independent. Upgrading or changing one layer does not affect the others. This means that if plugins change for all LAN cards, other elements, like the protocols, don't have to change.
  - The data link function of a LAN card provides hardware-level sending and receiving of network binary data. Zeros and ones flow from the network into the network card.
  - The card can recognize this flow and it can even check for errors.
  - When you turn on a computer with a LAN card, it will have two lights, one green and one orange.
  - The orange light will come on when the data link layer is activated.
  - This means that the cable works, there is a network connected, and data bits are flowing.
  - The second light, the green light, comes on once the next layer, the network layer (such as an IP network), is activated.

❖ Hub

- HUB is a hardware device that is used to network multiple computers together.
- A common connection point for devices in a network.
- Hubs are commonly used to connect segments of a LAN.
- A hub contains multiple ports.
- HUB sends information and broadcasts all network data across each connection.
- Hub can't make forwarding decision based on MAC address or IP address that's why when all computers received this packets, they simply check whether this packet is for them or not.
- If this packet is not for them they will discard it, except correct receiver.
- Most hubs can detect basic network errors such as collisions, but having all information broadcast to multiple ports can be a security risk.

Fig-2 Hub

- On the basis of its working methods, the Hubs can be divided into three types, given as:
    - Active Hub
    - Passive Hub
    - Intelligent /Smart Hub

- Passive HUB
    - Passive Hub works like a simple Bridge.
    - It is used for just creating a connection between various devices.
    - It does not have the ability to regenerate any incoming signal.
    - It receives signal and then forward it to multiple devices.

- Smart HUB
    - This is the third and last type of Hub.
    - It can perform tasks of both Active and Passive hubs.
    - Also, it can perform some other tasks like Bridging and routing.
    - It increases the speed and effectiveness of total network thus makes the performance of whole network fast and efficient.

- Active HUB
    - Active Hub is a hub which can amplify or regenerate the information signal.
    - This type of hub has an advantage as it also amplifies or regenerates the incoming signal as well as forwards it to multiple devices.
    - It can upgrade the properties if incoming signal before sending them to destination.
    - Distance between devices can be increase.
    - Active Hub is also known as Multi port Repeater.
    - More expensive then passive hub.

- Application of HUB
    - Networking Hub is widely used networking connectivity device.
    - It has many advantages over other connectivity devices.
    - Some Application of Networking Hub are given below:
        - Hubs are used to create small Home Networks.
        - Hubs are used for monitoring the networks.
        - Hubs are used in Organizations and Computer Labs for connectivity.
        - It makes one device or peripheral available throughout the whole network.

❖ Modem

- Modem is abbreviation for Modulator – Demodulator.
- A modem is a device that enables a computer to transmit data over telephone or cable lines.
- The computer network works in digital mode, while cable lines or telephone lines used analog technology for carrying massages, so modem converts between these two forms.
- Modem can transmit digital computer signals over telephone lines by converting them to analog signals.
- Modulator converts information from digital mode to analog mode at the transmitting end and demodulator converts the same from analog to digital at receiving end.
- The process of converting analog signals of one computer network into digital signals of another computer network is referred to as digitizing.
- Converting one signal from to another is called modulation.
- Recovering the original signal is called demodulation.

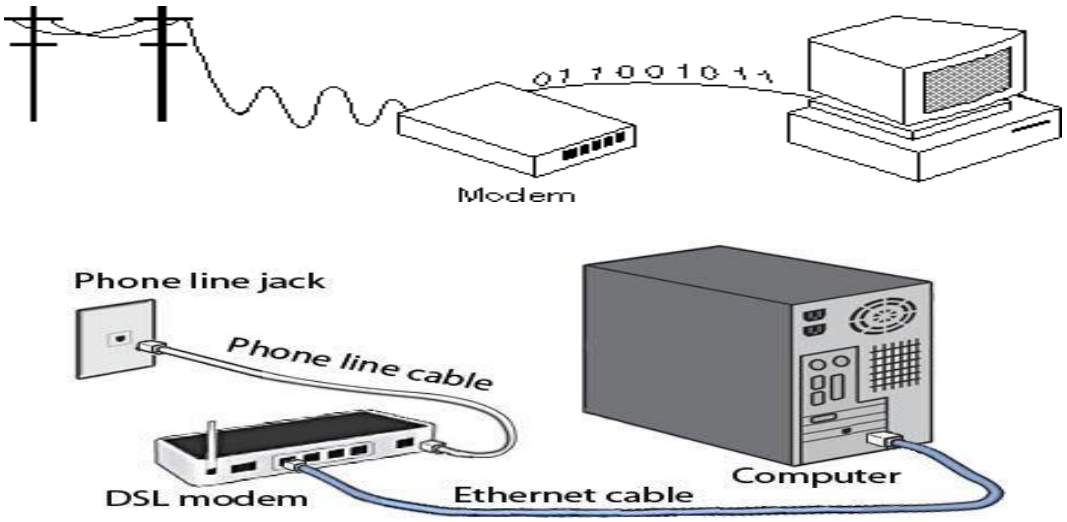


Fig-3 Connection of Modem

Fig-4 Modem

- Types of computer modems: Below are the three available versions of a computer Modem that can be used in computers.
  - Internal
  - External
  - Removable

- **Internal modem:** that connects to a PCI slot inside a newer desktop computer or an older computer.
- **External modem:** is located within a box and is hooked up externally to the computer, usually the Serial Ports or USB port.
- **Removable modem:** that is used with older laptops PCMCIA slot and is removed when you need the PCMCIA slot for another device.

a. Internal Modem b. External Modem c. Removable Modem

❖ DSL (Digital Subscriber Line / Loop)

- DSL Stands for "Digital Subscriber Line. "
- DSL is a communications medium used to transfer digital signals over standard telephone lines.
- Along with cable Internet, DSL is one of the most popular ways ISPs provide broadband Internet access.

- DSL is a high-speed Internet service like cable Internet.
- DSL provides high-speed networking over ordinary phone lines using broadband modem technology.
- DSL technology allows Internet and telephone service to work over the same phone line without requiring customers to disconnect either their voice or Internet connections.
- The bit rate of customer DSL services typically ranges from 256 Kbps to over 100 Mbps.

- Advantages of DSL:
  - You can leave your Internet connection open and still use the phone line for voice calls.
  - The speed is much higher than a regular modem
  - DSL doesn't necessarily require new wiring; it can use the phone line you already have.
  - The company that offers DSL will usually provide the modem as part of the installation.

- Disadvantages of DSL:
  - A DSL connection works better when you are closer to the provider's central office. The farther away you get from the central office, the weaker the signal becomes.
  - The connection is faster for receiving data than it is for sending data over the Internet.
  - The service is not available everywhere.

Internet Service	Upstream Speed (Upload)	Downstream Speed (Download)
DSL	128 Kbps to 384 Kbps	3 Mbps to 6 Mbps

❖ ADSL (Advanced Digital Subscriber /Line)

- Asymmetric digital subscriber line (ADSL) is a type of digital subscriber line (DSL) technology, a data communications technology that enables faster data transmission over copper telephone lines than a conventional voice band modem can provide.
- ADSL allows more data to be sent over existing copper telephone lines , when compared to traditional modem lines.
- ADSL supports data rates of from 1.5 to 24 Mbps when receiving data (known as the downstream rate or download speed) and from 1 to 5 Mbps when sending data (known as the upstream rate).
- Most ADSL communication is Full-duplex.
- Full-duplex ADSL communication is usually achieved on a wire pair by either Frequency-Division Duplex (FDD) or Time Division Duplex (TDD).

- How does ADSL broadband Work?

  - DSL is the name given to a broadband connection which works through the copper wires of your existing phone line.
  - When ADSL broadband is installed a micro filter is plugged into your phone connection.
  - This separates the frequency of your phone line from that of your broadband connection. It is this that allows you to surf the web while chatting on the phone.

- ADSL broadband comes through the phone line network direct to your house. This makes it the most popular type of broadband available, simply because it's so easy to sign up to.

Upstream Speed (Upload)	Downstream Speed (Download)	Distance Limit
1 Mbps to 5 Mbps	1.5 Mbps to 24 Mbps	9,000 feet to 18,000 feet

❖ Repeater

- The purpose of repeater is to extend the maximum range for the network.
- A repeater is a network device that repeats a signal from one port onto the other port to which it is connected.
- A repeater is an electronic device that receives a signal and retransmits it at a higher level and/or higher power, or onto the other side, so that the signal can cover longer distances.
- Repeater operates at OSI Physical Layer.

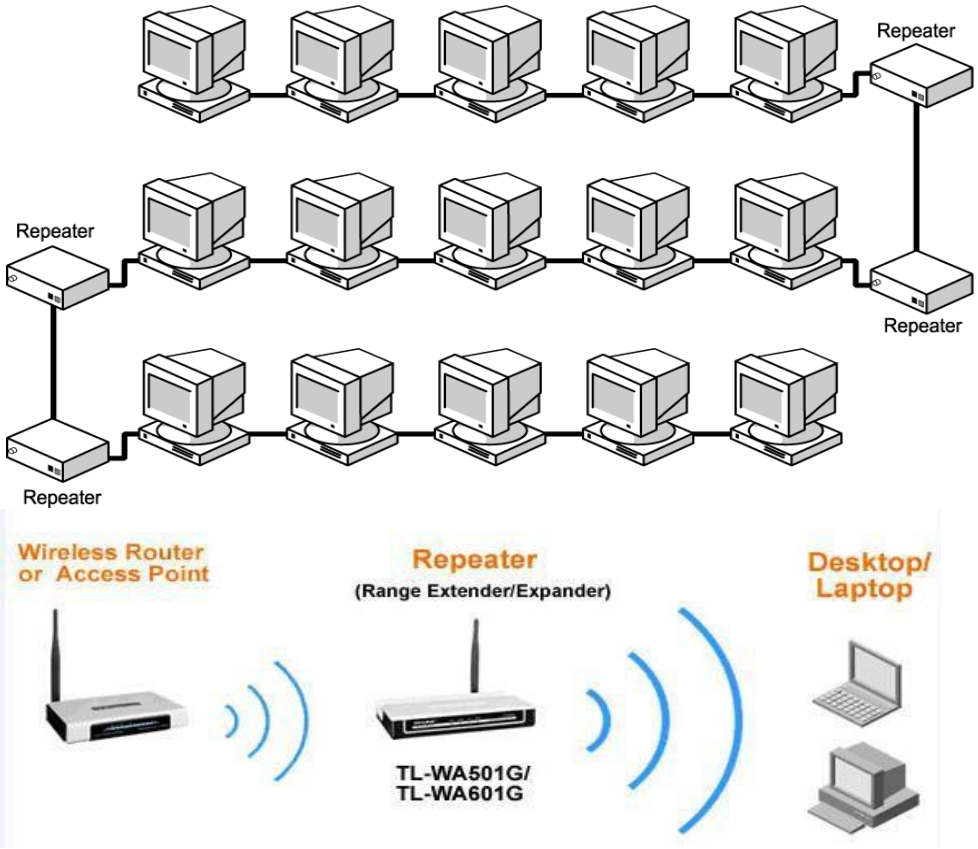


Fig-5 Work of Repeater

- A repeater is implemented in computer networks to expand the coverage area of the network, regenerate a weak or broken signal.
- Repeaters amplify the received/input signal to a higher frequency so that it is reusable and available.
- Repeater cannot require any addressing information.
- It is inexpensive and simple.

Layer 2 Devices

- Data Link Layer Devices are,
    - Bridges
        - Types of Bridge
            - Transparent Bridge
            - Translation Bridge
            - Source-route Bridge
    - Switches
        - Switching Methods
            - Cut-through method
            - Store and forward method
            - Fragment-free method
            - Multi speed Switches

❖ Bridges

- Bridges operate at the data link layer (Layer 2) of the OSI model.
- In telecommunication networks, a bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or token ring).
- A bridge device filters data traffic at a network boundary. Bridges reduce the amount of traffic on a local area network (LAN) by dividing it into segments.

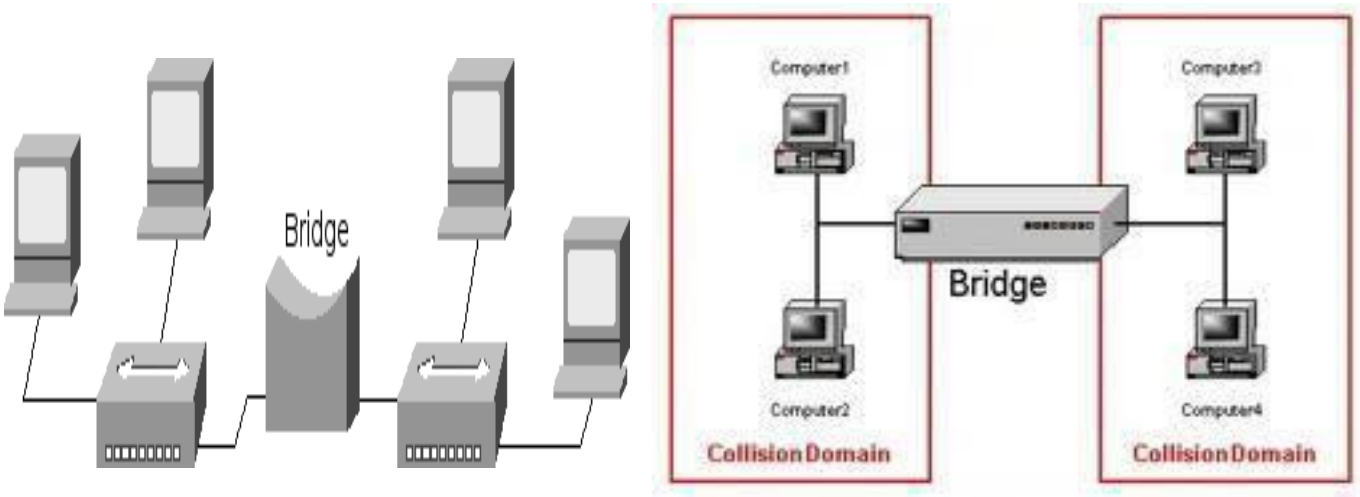


Fig-6 Bridge

- Bridges are classified as follows:
  - Local Bridge
  - Remote Bridge

- Local Bridges:
  - Used to directly connect multiple segments of the LAN.
  - For Example: A local bridge will be used to connect two departments that are located in the same building but on separate floor.

- Remote Bridge:
  - Used to connect multiple segments of the LAN, which are places in different locations.
  - For Example: A remote bridge will be used to connect two departments that are located in two different building.

- Types of Bridges:
  - Transparent Bridge
  - Translational Bridge
  - Source-route Bridge

- Transparent Bridges
  - Transparent Bridges is invisible to the other devices on the network.
  - Transparent Bridge only performs the function of blocking or forwarding data based on MAC address.
  - MAC address may also be referred as hardware address or physical address.
  - These addresses are used to build tables and make decision regarding whether a frame should be forward and where it should be forwarded.
  - Transparent Bridge is commonly used in Ethernet Networks.

- Translational Bridging
  - Translational Bridges are use full to connect segments running at different speeds or using different protocols such as token Ring and Ethernet networks.
  - The frame format differs depending on the type of network.
  - When data is transferred from one networking system to another, this bridge converts data depending on the network.
  - Depending on the direction of travel, a Translational Bridge can add or remove information and fields from frame as needed.

- Source-route Bridge
  - Source-route Bridges were designed by IBM for use on Token ring networks.
  - The S-r Bridge derives the entire route of the frame embedded/contained within the frame.
  - This allows the Bridge to make specific decision about how the frame should be forwarded through the network.
  - Each LAN consists of unique 12 bit number and each bridge consists of 4 bit number that uniquely specifies the path.

- Connect to bridge in network
  - Connect one end of the network cable to network port on the bridge.
  - Connect other end of the network cable to LAN port on the computer.
  - Connect power cable to the power connector of the bridge.
  - Connect other end of the power cable to a wall outlet or power strip.

❖ Switches

- A switch is a device used on a computer network to physically connect devices together. Multiple cables can be connected to a switch to enable networked devices to communicate with each other.
- Small switches generally have 24 ports capable of creating 24 different network segments for a LAN.
- Larger Switches may have hundreds of ports for creating LAN segments.
- Switch connects separate LAN segments.
- It allows multiple systems to transmit simultaneously.
- Working of switch
  - When switch receives data from one of the connected devices, it forwards data only to the port on which the destination system is connected.
  - It uses the Media Access Control (MAC) address of the devices to determine the correct port.
  - The cost of switches depends on the ports. As the number of ports increase, cost increase.

Fig-7 Switch Device

- Switching Methods: A switch uses one of the following methods to send data over the network.

  - Cut-through method
  - Store and forward method
  - Fragment free method

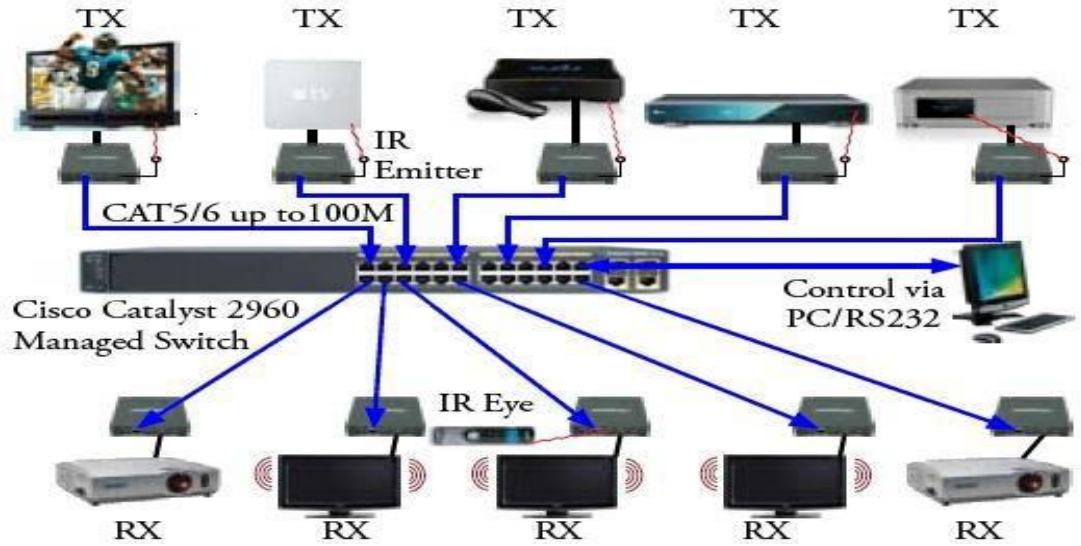


Fig-8 Work of Switching Device

- Cut-through method
  - Switch forward the packet as soon as receives.
  - Error checking is not performed on the packet in this method.

- Store and Forward method
  - The switch waits until it receives the entire packet and then starting forwarding.
  - It also performs basic error checking.
  - Store and forward method takes longer time then cut-through method.

- Fragment-free method
  - It works like cut-through method, accepts a switch in fragment-free method stores the first 64 bytes frame before forwarding.
  - The most network errors and collisions occur during the first 64 bytes of frame.
  - It is faster then cut-through method.

- Difference between bridge and switches
  - Bridges are used to connect smaller LAN segments while Switches are used to segments a large LAN into a smaller segments.
  - Bridges generally have few ports for LAN connectivity, while switches have many.
  - Bridges supports only store and forward while switches supports store and forward as well as manage signals flow and reduce network traffics.
  - It is more advanced then hub but not as advanced as router.

Layer 3 Devices

- Layer 3 devices are,
  - Router
  - Layer 3 Switches
  - BRouter
  - Network printer
  - Gateway

❖ Router

- A router is a device that forwards data packets along networks.
- A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network.
- Routers are located at gateways, the places where two or more networks connect.
- A router is hardware device designed to take incoming packet, analyze the packets, moving the packets to another network, converting the packets to another network interface, dropping the packets, directing packets to the appropriate locations, and performing any other number of other actions.
- A router has a lot more capabilities than other network devices such as a hub or a switch that are only able to perform basic network functions.
- The primary function of a router is to connect networks together and keep certain kinds of broadcast traffic under control.
- A router generally divides into two types.
    - A regular or normal router which is used to connects other routers.
    - A gateway router connects a single LAN to larger network usually to internet.
- For example, routers are commonly used in home networks to share a single Internet connection with multiple computers.
- Routing Table
    - Routers maintain routing tables that provide information about the path from router to destination.
    - These two commands are used to view routing table.
        - Netstat-n: used to display all the address and port numbers in the form of number.
        - Netstat-r : Used to display the routing table
- Routing operations
    - Depending on the destination, router selects the best path for the packet from its routing table.
    - There are two types of routers, static and dynamic
    - Static Routers:
        - Enables the network administrator to enter the route information manually in the routing table.
        - But the process is very time consuming.
        - It the topology of network changes, the router must be manually reconfigured.
        - Static routers are generally used only in the small networks.
    - Dynamic Router:
        - Update the routing table automatically according to the changes in network topology and information received from other router.
        - This process is not time consuming.
        - Dynamic router is used in the large network.

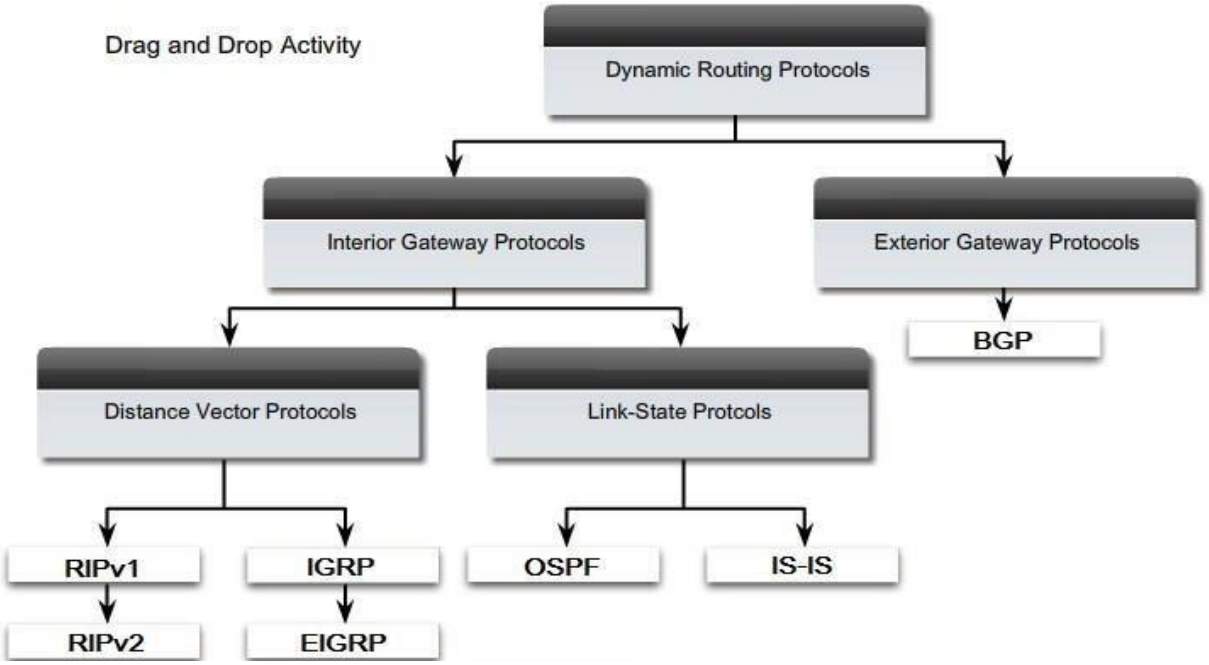


Fig-9: Dynamic Routing Protocols

- Routing Protocols
  - Router communities communicate with each other using routing protocols.
  - The Protocols helps routers to learn the network topology and changes that occur in the network topology.
  - Routing protocols use routing algorithms to decide the best output path for the received packet.

- Function of Router
  - Restrict broadcasts traffic to the LAN
  - Perform Protocol Translation (Wired Ethernet to Wireless / Wi-Fi , or Ethernet to CATV)
  - Move (route) data between networks
  - Calculate 'best paths' to reach network destinations.

❖ BRouter

- A BRouter is a device that functions as both a bridge and a router.
- It can forward data between networks (serving as a bridge), but can also route data to individual systems within a network (serving as a router).
- The main purpose of a bridge is to connect two separate networks. It simply forwards the incoming packets from one network to the next.
- A router, on the other hand, is more advanced since it can route packets to specific systems connected to the router.
- A BRouter combines these two functions by routing some incoming data to the correct systems, while forwarding other data to another network.

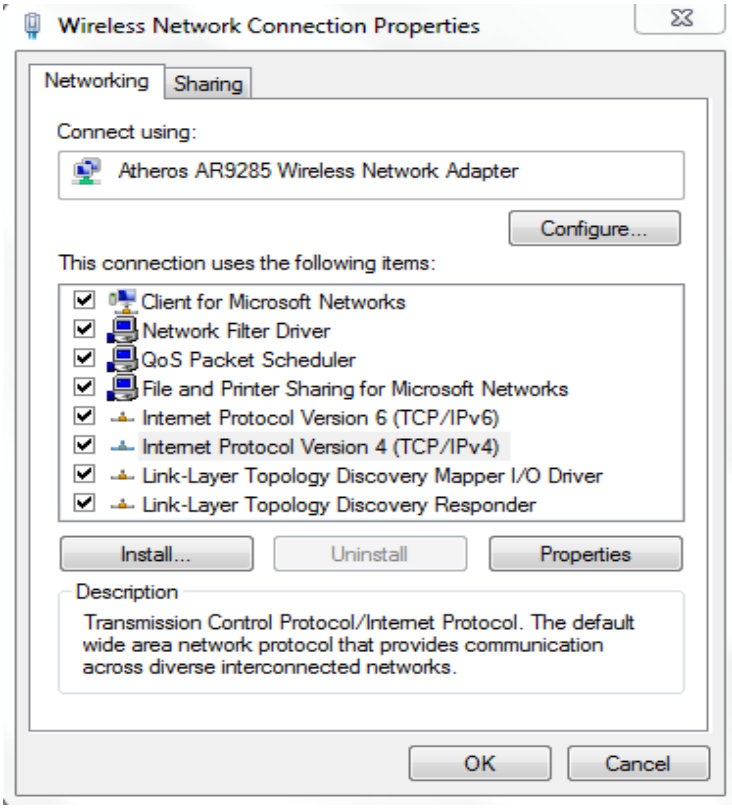
❖ Layer3 Switches

- A Layer 3 switch is a high-performance device for network routing.
- Layer 3 switches actually differ very little from routers.
- A Layer 3 switch can support the same routing protocols as network routers do. Both inspect incoming packets and make dynamic routing decisions based on the source and destination addresses inside.

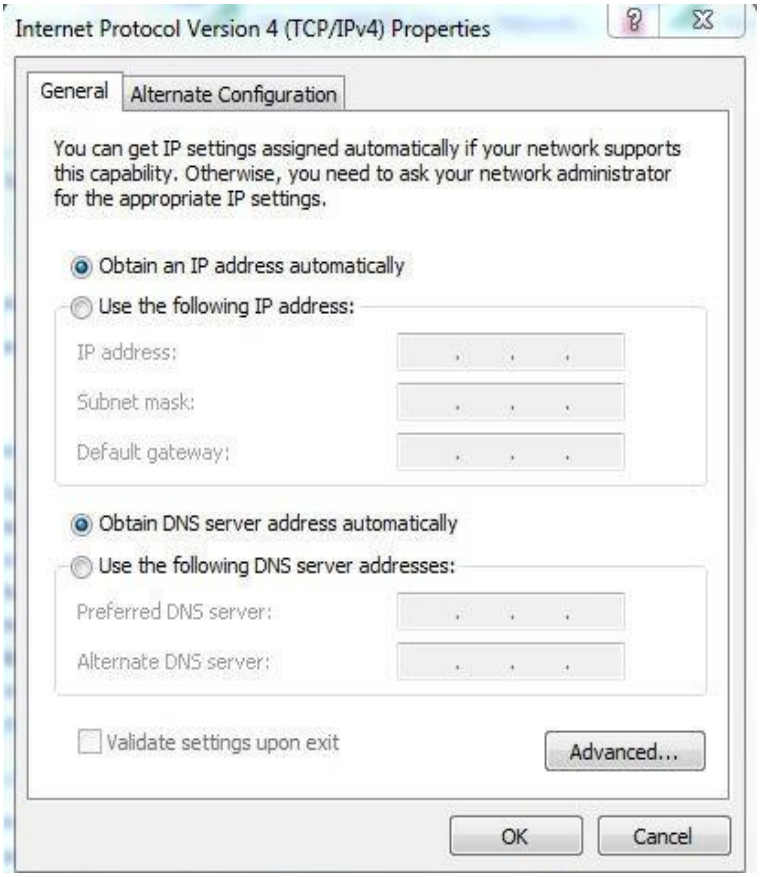
- Layer 3 switches a technology to improve on the performance of routers used in large local area networks (LANs) like corporate intranets.
- The key difference between Layer 3 switches and routers lies in the hardware technology used to build the unit.
- The hardware inside a Layer 3 switch merges that of traditional switches and routers, replacing some of a router's software logic with hardware to offer better performance in some situations.
- Layer 3 switches often cost less than traditional routers.
- Designed for use within local networks, a Layer 3 switch will typically not possess the WAN ports.

❖ Gateway

- A gateway is a network point that acts as an entrance to another network.
- 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.
- Gateway provides a connection between two networks. The networks do not need to use the same network communication protocol.
- In the network for an enterprise, a computer server acting as a gateway node is often also acting as a proxy server and a firewall server.
- A firewall keeps out unwanted traffic and.
- A proxy server is software that "sits" between programs on your computer that you use (such as a Web browser) and a computer server—the computer that serves your network.
- A gateway is often associated with both a router, which knows where to direct a given packet of data and a switch, which finds the actual path in and out of the gateway for a given packet.
- Depending on the types of protocols they support, network gateways can operate at any level of the OSI model.
- To configure a default gateway
  - To open Network Connections,
  - Click Start → Click Control Panel → Click Network and Internet Connections → Click Network Connections

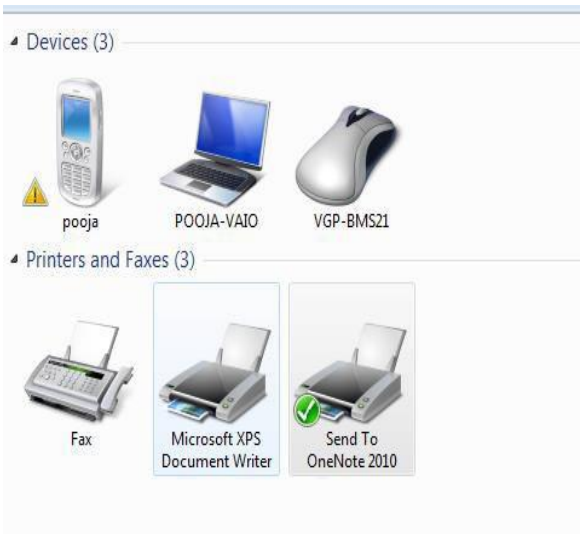


- Right click on network connection you want to change default gateway → Click on properties → Choose Internet Protocol (TCP/IP) → Clink on properties.



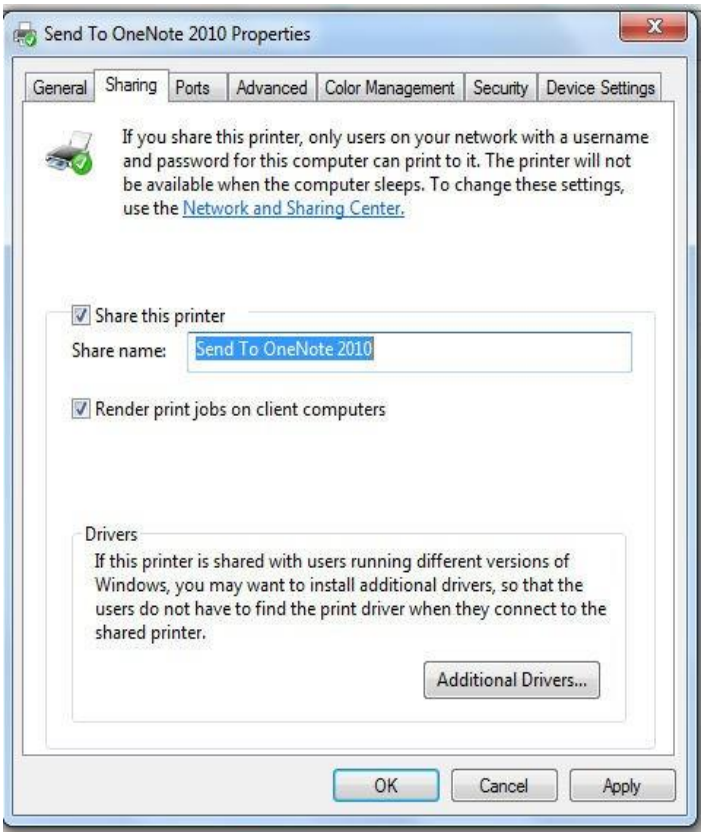
❖ Network Printer

- A class of printers, often called network printers, is specifically designed for connecting directly to a computer network. Larger businesses have for a long time integrated these printers into their company networks for their employees to share.
- Printer connected to a wired or wireless network. It may be Ethernet cable (wired) or it may connect to a Wi-Fi (wireless) network, or both.
- Host computer should go to install a new printer.
- It is easy to share a printer over the network.
- How to connect network printer?
  - Step 1: Click "Start" from task bar and then click on "Device and Printer Sharing" from the popup menu.



- Step 2: Open window that appears, select the printer you want to share and right click on it and select “Printer Properties”.

- Step 3: In the dialog box click on the tab “Sharing”. Then Put a check on the “Sharing this printer”. And writ a “Share name”.



- Step 4: Click “apply” and then click “Ok”.

Wireless network devices

- Wireless Network Devices are,
    - Wireless router
    - Wireless Switch
    - Access Point

❖ Wireless Router

- Wireless router is a device that performs the functions of a router but also includes the function of wireless access point.
- It is commonly used to provide access to the internet or other computer network.
- It does not required a wired link, as the connection is made wireless, via radio waves.
- A Wireless router is a small electronic device that allows you build a home network simply.
- The home router serves the core of the network to which computers, printers and other devices can be connected for example :
    - Share files between computers.
    - Share an Internet connection between computers.
    - Share a printer.
    - Connect your game console or other home entertainment equipment to the internet.
- Characteristics of wireless router.
    - One or more NIC supporting fast Ethernet.
    - Some wireless routers are also including an xDSL modem.
    - Some wireless routers operate the 2.5 GHz and 5 GHz bands simultaneously.
    - Some high wireless routers have data transfer rates of at most 300 Mbps and 450 Mbps.
    - Some wireless routers have a USB port specifically designed for connecting 3G mobile broadband modem.

❖ Wireless Switch

- Wireless switches connect to the access point through wired connections.
- They also connect to the enterprise network through their other switch ports.
- The wireless switch system ensures high system reliable and maximum mechanisms.
- In addition, In the unlikely event of a wireless switch failure, the system automatically fails over to backup device ensuring nonstop services.
- Wireless switch system reduce the cost of network manufacture which lower cost of managing, maintaining and upgrading the wireless infrastructure.
- Installation and maintenance cost are decreased because access point do not need manual configuration.

❖ Access Point

- In computer networking, a Access Point is a device that allows wireless device to connect to a wired networking using Wi-Fi or related standards.
- The AP usually connects to a router as a standalone device, but it also be an integral component of the router itself.

- Common AP Application

  - A hotspot is a common public application of APs, where wireless client can connect to the internet without regard for the particular networks to which they have attached for the moment.
  - A collection of connected hotspot can be referred to as a lily pad network.

- Security in AP

  - If wireless AP is connected to the network, anybody within range of the AP can connect to the network.
  - The most common solution is wireless traffic encryption.
  - Modem access points come with built in encryption.
  - The second and third generation WAP is considered secure, using a strong password.

Full Form

- LAN : Local Area Network
- DSL : Digital Subscriber Line/Loop
- ADSL : Advanced/Asymmetric Digital Subscriber Line
- NIC : Network Interface Controller
- USB : Universal Serial Bus
- PCI : Peripheral Component Interface
- Modem : Modulator – Demodulator
- FDD : Frequency-Division Duplex
- TDD : Time Division Duplex
- MAC : Media Access Control
- BGP : Border Gateway protocol
- IS-IS : Intermediate System to Intermediate System
- RIP : Routing Information Protocol
- OSPF : Open Shortest Path First
- EIGRP : Enhanced Interior Gateway Routing Protocol
- WI-FI : Wireless Fidelity

UNIT-3

Network Protocols
Network Routing

❖ Protocol

- A Protocol is pre-defined rules for data transfer between two different computers.
- A protocol is a standard used to define a method of exchanging data over a computer network such as local area network, Internet, Intranet, etc.
- Each protocol has its own method of how data is formatted when sent and what to do with it once receive, how that data is compressed or how to check for errors in data.
- The protocol defines the format and meaning of the data that are exchanged.
- The protocol also determines whether the network uses the peer-to peer or client/server architecture.
- Protocol Rules:
  - Addressing and Routing of messages
  - Error Detection
  - Recovery
  - Sequence and flow control

❖ Packet

- A packet is one unit of binary data capable of being routed through a computer network.
- A packet is a segment of data sent from one computer or device to another over a network.
- When any file is sent from one place to another over internet, the TCP/IP divides the file into “chunks” of an efficient size called Packet.
- Each of these packets is separately numbered and includes the internet address of the destination.
- The individual Packets for the given files may travel from the different routes through internet.
- A packet contains the source, destination, size, type, data, and other useful information that helps packet get to its destination and read.
- Packet contains following information with it,
  - The destination address
  - The source address
  - Total number of pieces
  - The sequence number needed to enable reassembly

❖ Connection Oriented Protocol

- A type of transport layer data communication service that allows a host to send data in a continuous stream to another host.
- The connection oriented service will guarantee that all data will be delivered to the other end in the same order as sent and without duplication.
- Communication proceeds through three well-defined phases:
  - connection establishment
  - data transfer

- Connection release.

- In this protocol receiver always provides the acknowledgement message to the sender.
- If receiver send acknowledgment message then it means that transmission successfully completed between sender and receiver.

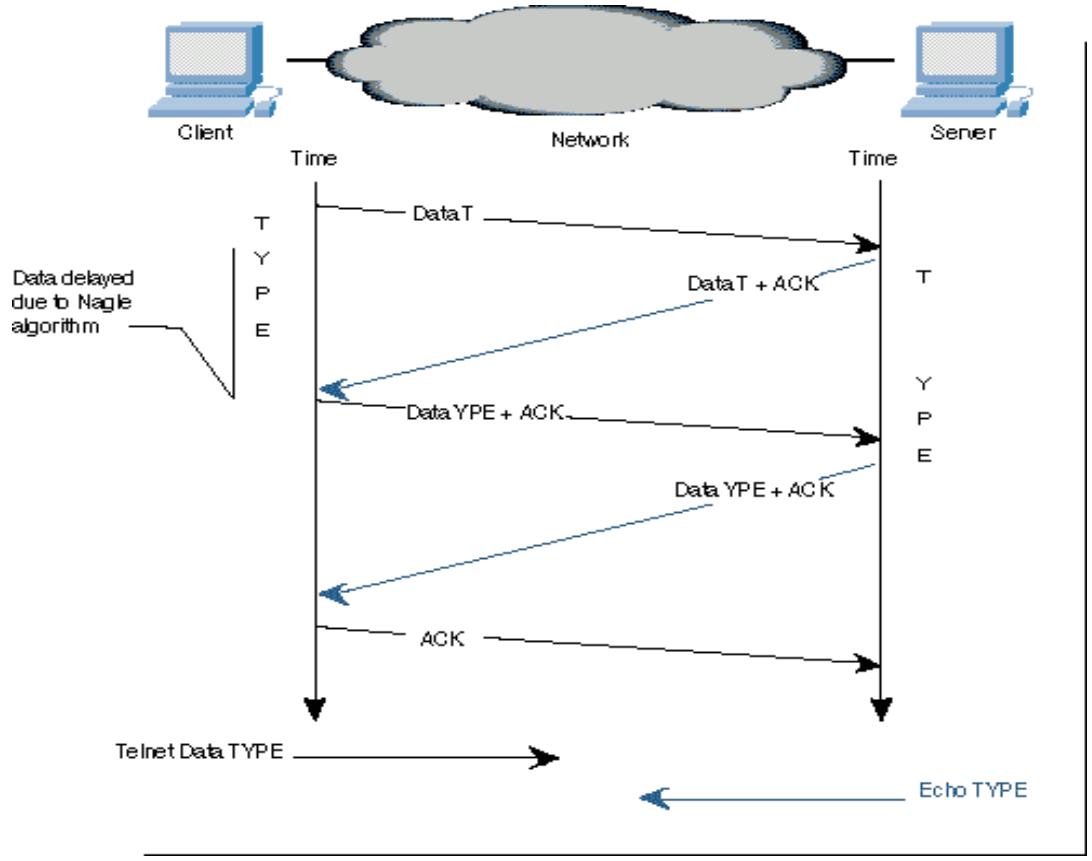


Fig-1: connection oriented protocol

- This protocol provides slow data communication speed because after completed each and every transaction receiver generate acknowledgment message to sender computer.
- In this sender computer is responsible for perfect data transfer process and receiver is responsible for acknowledgment message.
- The most common example is Transmission Control Protocol (TCP).
- Connection-oriented protocol service is sometimes called a "reliable" network service, because it guarantees that data will arrive in the proper sequence.
- Connection-oriented protocols are sometimes described as stateful protocol.
- COPs provide circuit-switched connections or virtual circuit connections.

❖ Connection less Protocol

- Connectionless describes communication between two network end points in which a message can be sent from one end point to another without prior arrangement.
- The device at one end of the communication transmits data to the other, without first ensuring that the recipient is available and ready to receive the data.
- The device sending a message simply sends it addressed to the intended recipient.
- If there are problems with the transmission, it may be necessary to resend the data several times.
- This type of protocol is not reliable and secure protocol.

- Sender only delivers data to receiver and sender has no worry about perfect data delivery.
- This protocol provides fast data communication speed because after completed each and every transaction receiver can not generate acknowledge message to sender computer.
- User Datagram Protocol (UDP) is an example of connection less protocol.

❖ TCP/IP Protocol Stack

- TCP/IP is a suite of protocols that can be used to connect dissimilar brands of computers and network devices.
- The largest network is Internet.
- The TCP/IP suite has become widely adopted, because it is an open protocol standard that can be implemented on any platform regardless of the manufacture.
- It is independent of any physical network hardware.
- TCP/IP can be implemented on Ethernet, x.25, Token passing among other platforms.
- The IP Portion of the TCP/IP is the connectionless network layer protocol.
- It is some time called an “unrealizable” protocol meaning that IP does not establish an end-to-end connection before packets and that it contains no error detection and recovery code.
- The TCP portion of the TCP/IP comes into operation once a packet is delivered to the correct internet address; TCP is Connection Oriented Protocol “reliable”.
- Another important TCP/IP protocol is the user datagram protocol (UDP).
- Like TCP UDP operates in transport layer.
- The major difference between TCP and UDP is that UDP is a connectionless protocol.
- UDP gives applications direct access to a Packet delivery service like IP service provides.
- TCP/IP protocol stack is a group of various protocols.
- In this protocol stack it includes following protocols,
  - HTTP (Hypertext Markup Language)
  - FTP (File Transfer Protocol)
  - SMTP (Simple Mail Transfer Protocol)
  - POP3 (Post Office Protocol)
  - SNMP (Simple Network Management Protocol)
  - Telnet
  - ARP (Address Resolution Protocol)
  - RARP (Reverse Address Resolution Protocol)

❖ HTTP (Hypertext Transfer Protocol)

- The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information system.
- Hypertext Transfer Protocol, HTTP is a set of standards that allow users of the World Wide Web to exchange information found on web pages.
- HTTP (Hypertext Transfer Protocol) is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.
- The Hypertext Transfer Protocol - provides a standard for Web browsers and servers to communicate.

- HTTP clients (such as Web browsers) and servers communicate via HTTP request and response messages.
- That's why all Web site addresses begin with "http://". Whenever you type a URL into your browser and hit Enter, your computer sends an HTTP request to the appropriate Web server.
- The Web server, which is designed to handle HTTP requests, then sends to you the requested HTML page.
- Basic Features of HTTP:
  - **HTTP is Connectionless:** The HTTP client, i.e., a browser initiates an HTTP request and after a request is made, the client disconnects from the server and waits for a response.
  - **HTTP is media independen**t: It means, any type of data can be sent by HTTP as long as both the client and the server know how to handle the data content.
  - **HTTP is stateless**: HTTP is connectionless and it is a direct result of HTTP being a stateless protocol. The server and client are aware of each other only during a current request. Afterwards, both of them forget about each other.
- History of HTTP:
  - The term HTTP was coined by Ted Nelson.
  - HTTP commonly utilizes port 80, 8008, or 8080.
  - HTTP/0.9 was the first version of the HTTP and was introduced in 1991.
  - HTTP/1.0 is specified in RFC 1945 and introduced in 1996.
  - HTTP/1.1 is specified in RFC 2616 and officially released in January 1997.

❖ Port Number

- A port number is part of the addressing information used to identify the senders and receivers of messages.
- These port numbers allow different applications on the same computer to share network resources simultaneously.

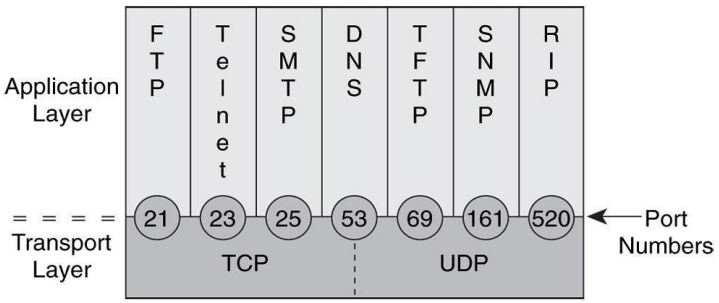


Fig-2: Port Number

❖ FTP (File Transfer Protocol)

- 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 client-server architecture and uses separate control and data connections between the client and the server.
- FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server (e.g., uploading a Web page file to a server).
- FTP used the port number 20 to data transfer and 21 to control data.

- If you are using a public--or anonymous--FTP server, you will not need proprietary sign-in information to make a file transfer, but you may be asked to enter your email address.
- If you are using a private FTP server, however, you must sign in with a user name and password to initiate the exchange of data.
- Your browser can also make FTP request to download programs you select from webpage.
- Using FTP you can also update (delete, rename, move, copy) files at server. You need to login to an FTP server.

❖ SMTP (Simple Mail Transfer Protocol)

- SMTP is part of the application layer of the TCP/IP protocol.
- Using a process called "store and forward," SMTP moves your email on and across networks.
- Simple Mail Transfer Protocol, a protocol for sending e-mail messages between servers.
- Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP.
- SMTP is generally used to send messages from a mail client to a mail server.
- SMTP is generally integrated within an email client application and is composed of four key components:
  - Local user or client known as the mail user agent (MUA)
  - Server known as mail submission agent (MSA)
  - Mail transfer agent (MTA)
  - Mail delivery agent (MDA)

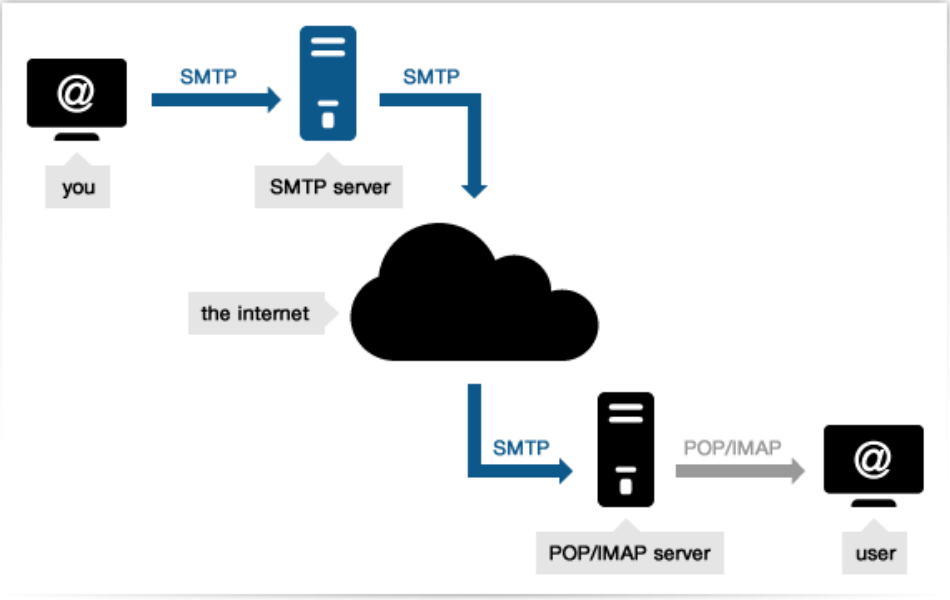


Fig-3: SMTP Protocol

- SMTP uses TPC port 25.
- SMTP directs how your email moves from your computer's MTA to an MTA on another computer, and even several computers, using that "store and forward" feature.
- Simple Mail Transfer Protocol is also known as RFC 821 and RFC 2821.

❖ POP3 (Post Office Protocol)

- Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client.
- POP3 allows you to download email messages on your local computer and read them even when you are offline.
- Most Email service provides such as Google Mail, Microsoft Mail and Yahoo! Mail provide both an IMAP (Internet Message Access Protocol) and POP3 service.
- POP3 uses port number 110.

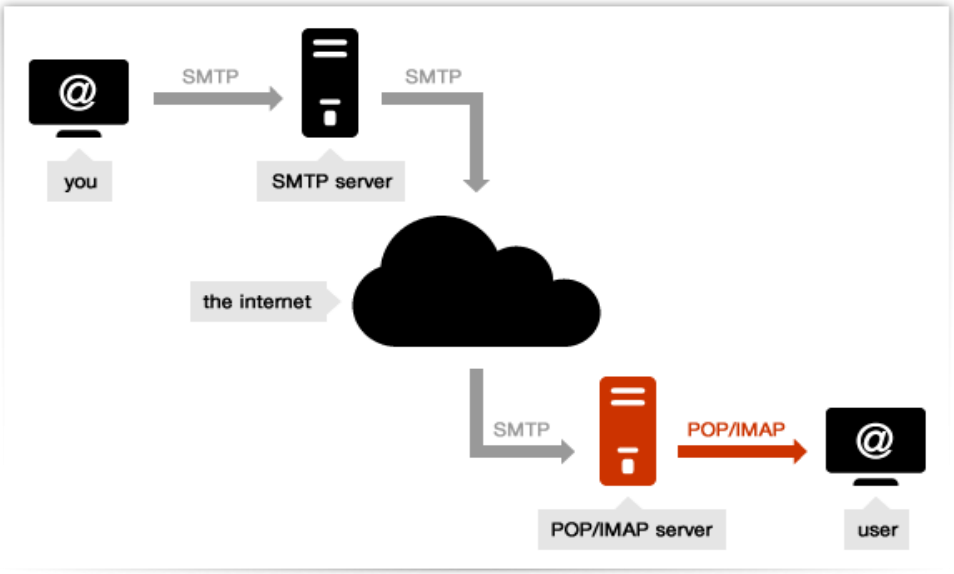


Fig-4 POP3 Protocol

- Advantages:
  - Email is available when you are offline
  - Email is not stored on the server, so your disk usage on the server is less
  - Just about any email client (software) supports POP3

- Disadvantages:
  - Can be much slower to check mail
  - Much harder to do server-side filtering
  - Mail is inaccessible from other machines

❖ SNMP (Simple Network Management Protocol)

- Simple Network Management Protocol (SNMP) is a popular protocol for network management.
- It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, modems and routers on an Internet Protocol (IP) network.
- The SNMP protocol is included in the application layer of TCP/IP as defined by the Internet Engineering Task Force (IETF).
- An SNMP managed network consist of 3 key components,

- Managed Devices:
  - A managed device is a network node that implements an SNMP interface that allows read-only, read-write access to node specific information.

- Agent – software which runs on managed devices
  - An agent is a network management software module that resides on a managed device.

- Network Management System (NMS) – software which runs on the manager
  - NMS executes applications that monitor and control managed device.

- The manager may send requests from any available UDP source port to port 161 in the agent.
- The manager receives notification on port 162.
- SNMP specifies five core Protocol Data Units (PDUs).
  - Get Request
  - Set Manager
  - GetNextRequest
  - Response
  - Trap

❖ TELNET

- Telnet is a client-server protocol based on a reliable connection-oriented transport layer protocol.
- The TELNET protocol provides a standardized interface, through which a program on one host (the TELNET client) may access the resources of another host (the TELNET server) as though the client were a local terminal connected to the server.
- It allows a user at one site to establish a TCP connection to a login server or terminal server at another site.
- A TELNET server generally listens on TCP Port 23.
- Most TELNET implementations do not provide you with graphics capabilities.
- TELNET is a protocol that provides "a general, bi-directional, eight-bit connection oriented communications facility".
- Telnet is a software program that supports the TELNET protocol over TCP.
- A TELNET protocol standard was defined at UCLA with the publication of two documents: Telnet Protocol Specification NIC #15372, and Telnet Option Specification, NIC #15373.
- Telnet was developed in 1969 beginning with RFC 15, extended in RFC 854, and Standardized as Internet Engineering Task Force (IETF).
- The word Telnet may also referred to the software that implements the client part of the protocol.
- 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.

❖ ARP (Address Resolution Protocol)

- Address Resolution Protocol, a network layer protocol used to convert an IP address into a physical address.

- The term address resolution refers to the process of finding an address of a computer in a network.
- The address resolution procedure is completed when the client receives a response from the server containing the required address.
- ARP was defined by RFC 826 in 1982. It is internet standard.
- ARP has been implemented in many type of networks such as IP network, Token Ring network, FDDI, DECENT, IEEE 802.11, ATM (Asynchronous Transfer Mode) and other LAN technologies.
- Announcement ARP also called a Gratuitous ARP message, is usually broadcast as an ARP request containing the sender's address in the target field with the target hardware address.
- The ARP protocol is a low level request and answer protocol that is communicated on the media access level of the underlying network.
- ARP has been implemented in many type of networks, such as Internet Protocol (IP) network, CHAOS, DECENT, Token Passing, FDDI, IEEE 802.11.
- An ARP probe is an ARP request constructed with an all-zero sender IP address.
- The term is used in the IPv4 address conflict Detection specification (RFC 5227).

❖ Apple Talk

- Apple Computer developed the AppleTalk protocol suite to implement file transfer, printer sharing, and mail service among Apple systems using the Local Talk interface built into Apple hardware.
- AppleTalk was included in the original Macintosh released in 1984.
- AppleTalk is used to connect Macs together in a Local Area Network (LAN).
- AppleTalk is a multi-layered protocol providing inter network routing, transaction, data transfer service, naming service and print sharing.
- Apple also produced other devices which can use AppleTalk for network communications, such as the LaserWriter, Servers to connect the LAN.
- Because of the popularity of the Internet and its use of TCP/IP, AppleTalk is no longer the default protocol for Apple systems.
- Support for AppleTalk was dropped in 2009 with the release of Mac OS X v10.6.
- Apple Talk originally supported networks of limited scope.
- The Apple Talk Phase-II specification issued in 1989, however, extended the scope of the Apple talk to enterprise networks.
    - Used only in Apple Networks
    - Routable Protocol
    - Apple Talk Phase II allows this protocol to work with others
    - Apple Talk divides groups of computers into zones instead of Domains

❖ NetBIOS Name Protocol

- NetBIOS (Network Basic Input/output System).
- NetBIOS was developed in 1983 by Sytek Inc. as a software communication over IBM PC Network LAN technology.
- Network Basic Input/output System. It provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a local area network.
- NetBIOS provides three distinct services:

- Name service (NetBIOS-NS) for name registration and resolution.
- Datagram distribution service (NetBIOS-DGM) for connectionless communication.
- Session service (NetBIOS-SSN) for connection-oriented communication.

- Assigning NetBIOS Names:
  - Every computer must have unique name.
  - The Computer name must be 15 characters longer or fewer.
  - NetBIOS name can include alphanumeric character and any of the following special characters.
  - NetBIOS names are not case-sensitive.
- Every Computer on a network must have a unique name for accessible on network.
- This unique name is called a computer name or NetBIOS name.
- This results in each computer in the network having both an IP address and a NetBIOS name corresponding to a host name.
- NetBIOS is not a networking protocol.

❖ L2CAP

- L2CAP (Logical Link Control and Adaptation Protocol).
- L2CAP provides connection oriented and connection less data services to upper layer protocols (HTTP, UDP, TCP, IP, FTP, TELNET) with multiplexing capacity, segmentation and reassembly operations.
- L2CAP has many/functions
  - Multiplexing between different higher layer protocols, allowing them to share lower layer protocols (ARP, FDDI, RARP, PPP)
  - 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 used by Bluetooth's higher layers.
  - Group management, providing one-way transmission to a group of other Bluetooth devices.

❖ RFCOMM (Radio Frequency Communication)

- RFCOMM is a simple set of transport protocols, made on top of the L2CAP protocol.
- RFCOMM is sometimes called serial port emulation.
- RFCOMM provides a simple reliable data communication to the user, similar to TCP.
- Many Bluetooth applications use RFCOMM because of its widespread support and publicly available on most operating systems.
- RFCOMM is used to transport the user data, modem control signals and configuration commands.
- The RFCOMM protocol supports up to 60 simultaneous connections between Bluetooth devices.
- TCP are concerned with having a point-to-point connection over which they can reliably exchange of data.
- If a portion of that data cannot be delivered within a fixed time limit, then the connection is terminated and an error is delivered, RFCOMM provides the same major attributes of TCP.

❖ IPX/SPX

- Inter network Packet Exchange/Sequenced Packet Exchange (IPX/SPX) is a set of network protocols that provide packet switching and sequencing for small and large networks.
- It was created by Novell Inc. primarily for Novell NetWare networks, but is popular enough that it is used on products that are not from Novell.
- IPX/SPX is generally smaller and faster then TCP/IP.

  - IPX – Inter network Packet Exchange supports the transport and network layers of the OSI network model. Provides for network addressing and routing. It provides fast, unreliable, communication with network nodes using a connection less datagram service.
    - Connection less protocol
    - Resides at network layer
    - Responsible for network addressing and routing.

  - SPX - Sequenced Packet Exchange operates at the transport layer providing connection oriented communication.
    - Connection oriented protocol
    - Resides at the transport layer
    - Uses service provided by IPX
    - Reliable data transfer
- Advantages of IPX/SPX
  - Used mostly in Novell Netware networks.
  - Not supported on the internet
  - Typically found in private network

❖ RARP (Reverse Address Resolution Protocol)

- The Reverse Address Resolution Protocol (RARP) is a computer networking protocol used by a client computer to request its Internet Protocol (IP) address from a computer network.
- RARP is a protocol by which a physical machine in a local area network can request to its IP address from a server's Address Resolution Protocol (ARP) table or cache.
- RARP is described in Internet Engineering Task Force (IETF) publication RFC 903.
- 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 requires one or more server hosts to maintain a database of mappings of MAC addresses to their respective IP addresses.
- Reserves ARP differs from the Inverse Address Resolution Protocol (InARP) describe 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.

❖ Quick Overview

- **HTTP:** Provides a Standard for web browsers and servers to communicate. (Exchange information found in web pages).
- **FTP:** Download a file from server and upload a file to server.
- **SMTP:** Sending an email from client machine to appropriate server.
- **POP3**: Receivers an email from server to local email client.
- SNMP: Collecting information from network devices such as server, printer, hub, switches, modem, and routers on an internet.
- **TELNET**: Program on one host may access the resources of another host.
- **ARP:** ARP refers to the process of finding an address of a computer in network.
- **RARP**: Used by client computer to request its IP address from computer network.
- **Apple Talk**: Used in Mac system for file transfer, printer sharing, sending and receiving a mail, etc.
- **NetBIOS:** Providing 3 services, Name service, Datagram Service and Session Service.(Application on separate Computer to communicate over a LAN)
- **L2CAP**: Used upper layer protocol with multiplexing, segmentation and reassembly option.(Bluetooth)
- **RFCOMM:** Work Like TCP Protocol (Bluetooth)
- **IPX/SPX**: Packet Switching and sequencing for small and large network.(Novell NetWare OS)

Full Form

- HTTP : Hypertext Markup Language
- FTP : File Transfer Protocol
- SMTP : Simple Mail Transfer Protocol
- POP3 : Post Office Protocol
- SNMP: Simple Network Management Protocol
- PDU : Protocol Data Units
- RARP:Reverse Address Resolution Protocol
- IPX : Inter network Packet Exchange
- SPX: Sequenced Packet Exchange
- RFCOMM : Radio Frequency Communication
- L2CAP : Logical Link Control and Adaptation Protocol
- NetBIOS :Network Basic Input/output System
- IETF : Internet Engineering Task Force
- RFC : Request For Comment

Network Routing

What is Routing?

- Routing is the process of selecting best paths in a network.
- Routing is usually performed by a dedicated device called a router.
- Routing is performed for many kinds of networks, including the telephone network (circuit switching), electronic data networks (such as the Internet), and transportation networks.
- This Unit is concerned with routing in electronic data networks using packet switching technology.

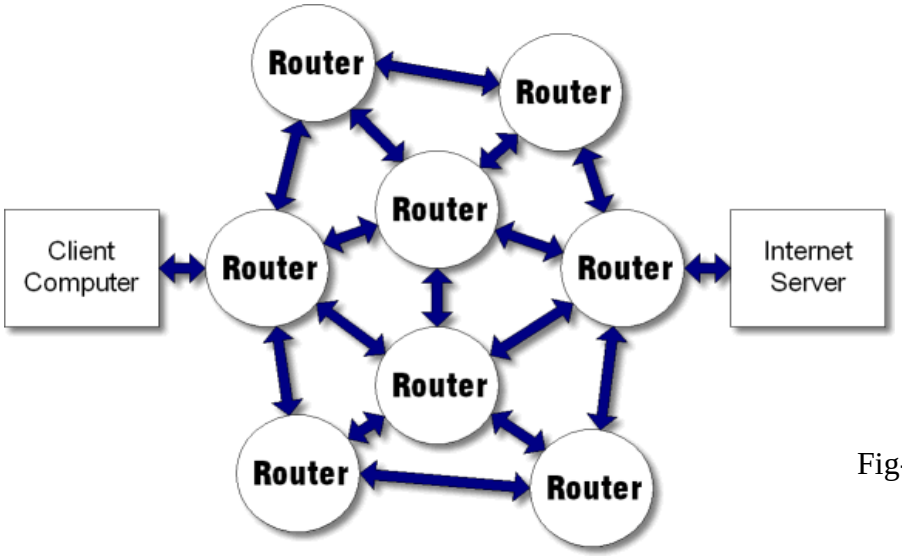


Fig-1: Routing

- In packet switching networks, routing directs packet forwarding (the transit of logically addressed network packets from their source toward their ultimate destination) through intermediate nodes.
- Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, or switches.
- The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations.
- Routers maintain routing tables that provide information about the path from router to destination.
- These two commands are used to view routing table.
    - Netstat-n: used to display all the address and port numbers in the form of number.
    - Netstat-r : Used to display the routing table
- Most routing algorithms use only one network path at a time.
- In case of equal routes, the following elements are considered to decide which routes get installed into the routing table:
    - Prefix-Length: independent of whether it is within a routing protocol or over different routing protocol
    - Metric: where a lower cost is preferred
    - Administrative distance: where a lower distance is preferred

Requirements of Routing

- Routing is the process of sharing data between two different LAN.
- It requires sharing information between various networks.
- To select best routs from sender and receiver
- To require to specify topology distribution in network.
- To specify metrics, administrative distance and delivery semantics.

1. Delivery semantics:

- Routing semantics differ in their delivery semantics.
- Unicast delivers a message to a single specific node.
- Broadcast delivers a message to all nodes in their network.
- Multicast delivers a message to a group of nodes.
- Anycast delivers a message to anyone out of a group of nodes. (Typically one of the nearest to the source)
- Geocast delivers a message to a geographic area.

2. Topology Distribution:

- Static Routing small networks may use manually configured routing tables.
- Large networks have complex topologies that can change rapidly, making the manual construction of routing tables not possible.
- Most of the PSTN (Public Switched Telephone Network) uses Adaptive routing or Dynamic Routing.
- Dynamic routing constructs routing table automatically, based on information carried by routing protocols.

3. Administrative Distance:

- A network can use more than one routing protocol.
- Routers need to find a way to select a better path.
- Administrative Distance number is used by routers to find out which route is batter (Lower number is batter).
- For example some route use RIP and EIGRP, then router chooses EIGRP route, because EIGRP routes have by default administrative distance of 90, while RIP have 120.

Routing Protocol	Administrative Distance Value
• Static Route	1
• RIP (Routing Information Protocol)	120
• IGRP (Interior Gateway Routing Protocol)	100
• EIGRP (Enhanced Interior Gateway Routing Protocol)	90
• OSPF (Open Shortest Path First)	110
• IS-IS (Intermediate System Intermediate System)	115
• BGP (Border Gateway Protocol)	200

4. Router metrics:

- Router metrics can contain any number of values that help the router to determine the best route among multiple routes to a destination.
- A router metric typically based on information like path length, bandwidth, path cost, delay, communication cost.

Types of Routing

- There are three types of routing,
  1) Static Routing 2) Dynamic Routing 3) Default Routing

1. Static Routing

- A static routing table is created, maintained, and updated by network administrator manually.
- It is the manual configuration and selection of a network route, usually managed by the network administrator.
- Router will not share static router with each other, thus reducing CPU/RAM usages and saving bandwidth.
- If any changes in routing infrastructure, static routing requires manually intervention.
- Static routing can be used for small networks that require only one or two routes.
- Advantages:
  - Minimum CPU/Memory load
  - No speed overhead (Updates are not shared between routers)
  - Administrator control on how traffic is routed.
- Disadvantages:
  - Human Error: Administrators can make mistakes and mistype in network information, or configure incorrect routing paths by mistake.
  - Fault Tolerance: This means that when there is a change in the network or a failure occurs between two statically defined devices, traffic will not be re-routed.
  - Administrative overhead: Static routes must be configured on each router in the network(s). This configuration can take a long time if there are many routers.
  - Not Useful in large network

2. Dynamic/Adaptive Routing

- A router with dynamically configured routing tables is known as a dynamic router.
- Dynamic routing consists of routing tables that are built and maintained automatically through an ongoing communication between routers.
- A dynamic routing table is created, maintained and updated by routing protocol running on the router.
- Dynamic routing uses multiple algorithms and protocols. The most popular are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).
- Router does share dynamic routing information with each other, which increases CPU, RAM and bandwidth usages.
- Dynamic router automatically choosing a different path when there is a changes to the routing infrastructure.
- Advantages:
  - Simple to Configure on large network
  - Will dynamically choose best path
  - If Traffic increases it will able to balance between multiple links.
- Disadvantages:
  - Updates are shared between routers, thus consuming Speed
  - Routing protocol requires an additional load on router CPU/RAM.
  - “Best route” is defined by routing protocol.

3. **Default Routing**
   - If a specific route to a particular network does not exist, router will drop all traffic to network.
   - A default route/gateway allows traffic to be forwarded, even without a specific route to a particular network.
   - The default route is identified by all Zeroes in both the network and subnet.
   - The device to which the default route point is often called the default gateway.

Routing Protocols

- The purpose of routing protocol is to learn of available routes that are exits on the entire network, build routing tables and make routing decisions.
- Some of the most common routing protocols include IGRP, EIGRP, OSPF, IS-IS, BGP.
- Routing protocols divides into two types,
  - Interior Routing Protocol
  - Exterior Routing Protocol.
- Interior routing protocol includes static and dynamic routing procedure.
- Static interior routing done by administrator, but dynamic routing divided into three types.
  - Distance-vector protocols (RIP, IGRP)
  - Link-state protocols (OSPF, IS-IS)
  - Path vector (EIGRP)
- Exterior routing protocols includes BGP and EGP routing protocols.

Interior Routing Protocols

- WE discuss here Link state routing protocols, distance vector routing protocols and path vector routing protocols.

Distance-vector Routing

- Distance vector algorithms use the Bellman-Ford algorithm for calculating distance.
- This approach assigns a Distance/Cost number to each of the links between each node in the network.
- Node will send information from point A to point B via the path that result in the lowest total distance/cost.
- The algorithm operates in a very simple manner.
- When a node first starts, is only knows of its immediate neighbors, and the direct distance/cost involved in reaching them.
- All the nodes in the network will find the best next hop for all destinations, and the best total distance/cost.
- Updates of the full routing table are sent to routing neighbors.
- Neighbor will add the routes from these updates to their own routing tables.
- Each neighbor trusts this information completely, and will forward full routing table to every other neighbor.
- Router fully (blindly) rely on neighbor for route information, a concept known as routing by rumor.
- Distance vector routing used two protocols from routing protocols.

- RIP (Routing Information Protocols)
- IGRP (Interior Gateway Routing Protocols)

1. RIP (Routing Information Protocols)

- RIP is a standardized distance-vector protocol, designed for use on smaller network.
- RIP is a dynamic protocol used to find the best route or path from source to destination over a network by using a routing metric/hop count algorithm.
- This algorithm is used to determine the shortest path from the source to destination, which allows the data to be delivered at high speed in the shortest time.
- RIP uses a round robin system of load-balancing between equal matrices routes, which can lead to pinhole congestion.
- RIP sends out the full routing table every periodic update.
- Routing updates are sent via multicast, using 224.0.0.9
- RIPv1 routers will send only version 1 packets.
- RIPv1 routers will receive both version 1 and 2 updates.
- RIP2 routers will both send and receive only version 2 updates.
- Characteristics:
  - Distance-vector
  - Protocols: IP and IPX routing.
  - Update timer : 30 seconds
  - Hop count : 15
  - Administrative Distance: 120
  - Two Versions: Version 1 (RIPv1) and Version 2 (RIPv2).

2. IGRP (Interior Gateway Routing Protocol)

- IGRP is a distance-vector routing protocol developed by Cisco system for routing multiple protocols across small and medium sized Cisco networks.
- It is requires that you use Cisco routers.
- IGRP uses less bandwidth then RIP.
- Characteristics:
  - Distance-vector
  - Protocols: IP, IPX, Decent, Apple talk
  - Update timer : 90 second
  - Hop count : 100
  - Load balancing across 6 equal paths.

Link-state Routing

- Each router learns about its own links (directly connected networks)
- Find directly connected neighbors
- Each router uses the database to construct a complete map of the network topology
- Computes the best path to each destination network
- To find shortest path Dijkstra's algorithm is used.

- Link-state routing maintains 3 separate tables.
  - Neighbor Table: Contain a list of all neighbors.
  - Topology Table: contains a map of all links within an area. (also known as “link-state”)
  - Shortest Path Table: contains the best route to each particular destination. (also known as “routing Table”)
- Link state routing used two protocols from routing protocols.
  - OSPF (Open Shortest Path First)
  - IS-IS (Intermediate System to Intermediate System)

3. OSPF (Open Shortest Path First)

- Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks.
- It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS).
- OSPF is perhaps the most widely used in large enterprise networks.
- It gathers link state information from available routers and constructs a topology map of the network.
- OSPF supports Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) networks.
- OSPF detects changes in the topology, such as link failures, and converges within seconds.
- It computes the shortest path tree for each route using a method based on Dijkstra's algorithm, a Shortest Path First (SPF) algorithm.
- The Hello Packets contains information such as router timers, router ID and subnet mask.
- Hello Packets are used as a form of greeting, to allow a router to discover other adjacent routers (neighbor) on its local links and networks.
- The Packets/messages establish relationships between neighboring devices (called adjacencies) and communicate key parameters about how OSPF is to be used in the autonomous system or area.
- Characteristics:
  - Link-state
  - Hop count: none (Limited by network)
  - Load balancing across 4 equal paths
  - Hello timer: 10 seconds for Ethernet and 30 seconds for Non-Broadcast
  - Dead timer: 40 seconds for Ethernet and 120 seconds for Non-Broadcast

4. IS-IS (Intermediate System to Intermediate System)

- Intermediate System to Intermediate System (IS-IS) is a routing protocol designed to move information efficiently within a computer network, a group of physically connected computers or similar devices also known as DECnet Phase V routing,.
- It accomplishes this by determining the best route for packets through a packet-switched network.
- IS-IS use a area structure with level 1 and level 2 router types.
- Level 1 which has no direct connection outside of its area.
- Level 2 routers area which connects different areas.
- IS-IS must have an assigned address that is unique for that routing domain.
- An address format is used which is comprised of an area ID and a System ID.
- The Area ID is assigned area number and the System ID is a MAC address of one of device.

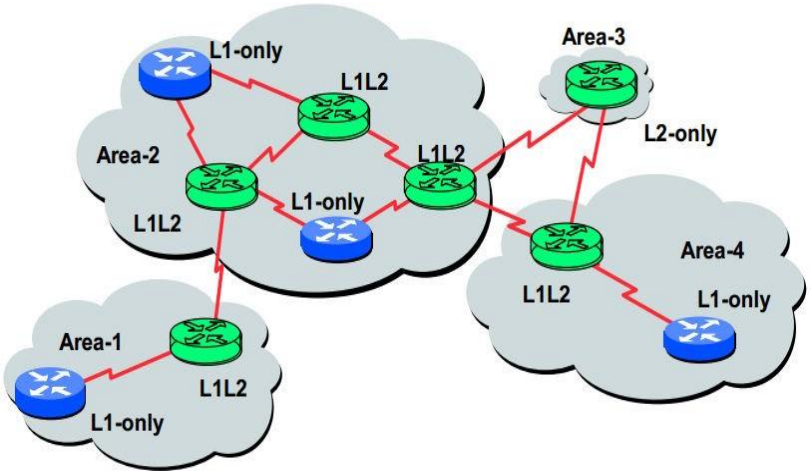


Fig-2: IS-IS L1 & L2 network

- Characteristics:
  - Link-state
  - Routes IP
  - Hop count: None (limited by network)
  - Load balancing across 6 equal paths
  - Hello timer: 10 seconds
  - Dead timer: 30 seconds

Distance-vector Routing	Link-state Routing
Sends the entire routing table	Sends only link state information
Slow coverage	Fast coverage
Updates are sometimes sends using broadcast	Always uses multicast for routing information
Don't know the network topology	Knows the entire network topology
Simple to configure	Can herder to configure
Protocols: RIP, IGRP	Protocols: OSPF, IS-IS

Autonomous System

- On the Internet, an autonomous system (AS) is the unit of router policy, either a single network or a group of networks that is controlled by a common network administrator (or group of administrators) on behalf of a single administrative entity (such as a university, a business enterprise, or a business division).
- Each autonomous system assigns an AS (Autonomous System) number.

Path-vector Routing

- Distance vector and link state routing are both intra-domain routing protocols, they used inside an autonomous system, but not between autonomous system.
- Path vector routing is similar to distance vector routing.
- A path vector protocol is a computer network routing protocol which maintains the path information that gets updated dynamically.
- In path vector routing we assume that there is one node in each autonomous system which acts on behalf of the entire autonomous system.
- This node is called the speaker node.
- The speaker node creates a routing table and advertises it to neighboring speaker nodes in neighboring autonomous system.
- Path vector routing is discussed in RFC 1322.

5. EIGRP (Enhanced Interior Gateway Routing Protocol)

- EIGRP is hybrid routing protocol developed by Cisco system for routing many protocols across an enterprise cisco network.
- It has many characteristics of both distance vector and link state routing protocols.
- It requires the cisco routers.
- EIGRP will route the same protocols the IGRP routes and use the same metrics as IGRP to select the best path.
- EIGRP is faster, it uses an algorithm called dual update algorithm or DUAL, which run when router detects that a particular routes is unavailable.
- This defined as a neighbor with a least cost route to a particular destination.
- If route changes are advertised only to affected routers when changes occur.
- Characteristics:
  - Advanced Distance vector
  - Routes IP, IPX, Decent, AppleTalk
  - Metrics: Bandwidth, Delay Load, Reliability
  - Hop count:255
  - Load balancing across 6 Equal paths
  - Hello timer :5 seconds on Ethernet/ 60 seconds on Non-Broadcast
  - Hold timer : 15 seconds on Ethernet / 180 seconds on Non-Broadcast

Exterior Routing Protocols

- Exterior Routing Protocol is 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 unlike modern distance vector and path vector protocols, it is limited to tree-like topology.
- BGP (Border Gateway Protocol) is Example of Exterior routing protocol.

6. BGP (Border Gateway Protocol)

- BGP is an exterior routing protocol.
- BGP routes between autonomous systems, which are assigned a particular AS number.
- AS numbers can be assigned to an office with one or several BGP routers.
- The BGP routing table is comprised of destination IP addresses, an associated AS-Path to reach that destination and next hop router address.
- BGP will route packets across an ISP network, which is a separate routing domain that is managed by them.
- A unique AS number assignment is required for customers when they connect unique BGP.
- There are 10 defined attributes that have a particular order or sequence, which BGP utilized as metrics to determine the best path to a destination.
- Each BGP router can be configured to filter routing broadcasts with route maps instead of sending/receiving the entire internet routing table.
- Characteristics:
  - Path vector
  - Routes IP
  - Hop count : 255
  - Load balancing across 6 Equal cost path
  - Alive Timer : 60 seconds
  - Hold down Timer: 180 seconds

Full Form

1. IRP: Interior Routing Protocol
2. ERP: Exterior Routing Protocol
3. RIP: Routing Information Protocol
4. IGRP: Interior Gateway Routing Protocol
5. EIGRP: Enhanced Interior Gateway Routing Protocol
6. OSPF: Open Shortest Path First
7. IS-IS: Intermediate System Intermediate System
8. BGP: Border Gateway Protocol
9. AS: Autonomous System
10. SPF: Shortest Path First
11. ISP: Internet Service Provider

Unit-4

IP Addressing
And
Windows 2008

What is IP Address?

- A unique string of numbers separated by full stops that identifies each computer using the Internet Protocol to communicate over a network.
- An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication

- IP address is used to identify device on a network.
- For example IP address is 11000000.10101000.00110110.11001001 in binary format but generally we denote in doted decimal i.e. 192.167.38.1.
- Each of the decimal numbers in an IP address is called an octet.
- So in this IP address first octet is 192, second octet 167 and so on.
- The range of decimal number in each octet varies from 0 to 255.
- AN IP address assigned to a computer may either b permanent address or temporary address.

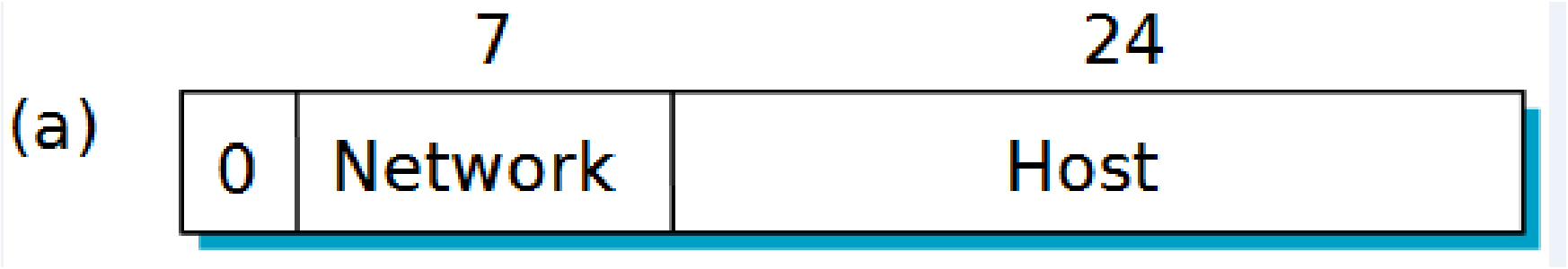
- IP address divided in two category,
  - Dynamic IP Address:
    - Dynamic IP address are assigned to the devices that require temporary connectivity to the network or non permanent devices.
    - The most common protocol used for assigning Dynamic IP address is DHCP (Dynamic Host Configuration Protocol).
      - For Example : Network Printer
  - Static IP Address:
    - Static IP address assigns to the devices on the network whose existence in the network remains for a longer duration.
    - These IP addresses are semi-permanent IP addresses which remains allocated to a specific device for longer time.
      - For Example :server

- IPV 4
  - Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP) Internet, and routes most traffic on the Internet.
  - IPV 4 is 32 bit number represented in a 4 decimal numbers, where each decimal number is 8 bit (an octet), where each octet is separated by a dot in between.
  - Thus the representation is knows as Doted Decimal Notation.
  - IPV4 has unicast, multicast and broadcast addresses.
  - Routing protocols that supports IPV4 addressing are RIPV1, RIPV2 IGRP, OSPF and EIGRP.

IP Address Classes IPV 4

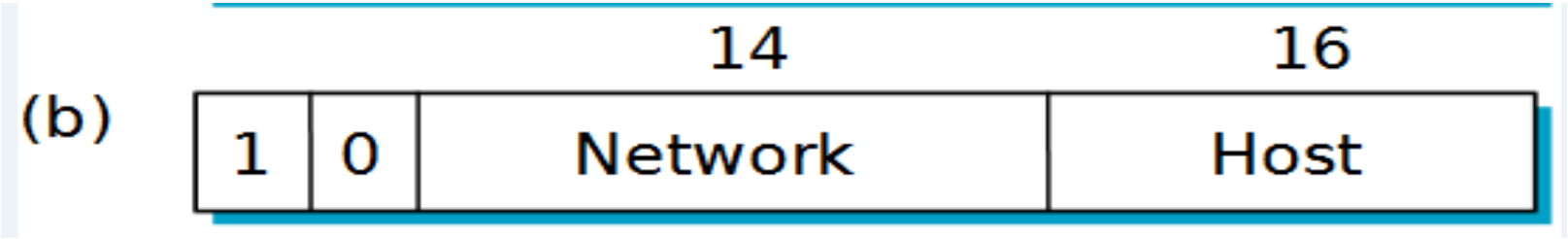
- The Scheme of IP addressing using address classes is called classful addressing.
- There are five classes of available IP ranges: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are commonly used.
- Each class allows for a range of valid IP addresses.

- Class A
  - Class A addresses are assigned to networks with a very large number of hosts.
  - The high-order bit in a class A address is always set to zero.
  - The next seven bits (completing the first octet) complete the network ID.
  - The remaining 24 bits (the last three octets) represent the host ID.



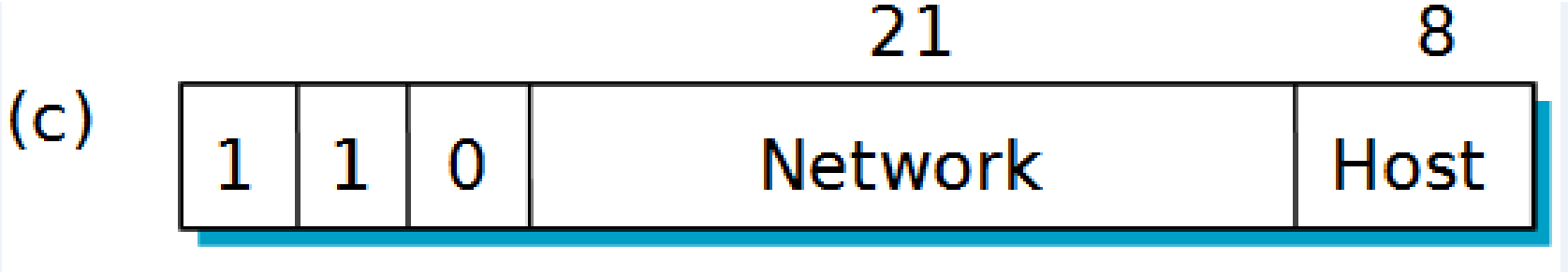
- The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.
- Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only.
- The IP range 127.x.x.x is reserved for loopback IP addresses.
- The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2).

- Class B
  - Class B addresses are assigned to medium-sized to large-sized networks.
  - The two high-order bits in a class B address are always set to binary 1 0.
  - The next 14 bits (completing the first two octets) complete the network ID. The remaining 16 bits (last two octets) represent the host ID.



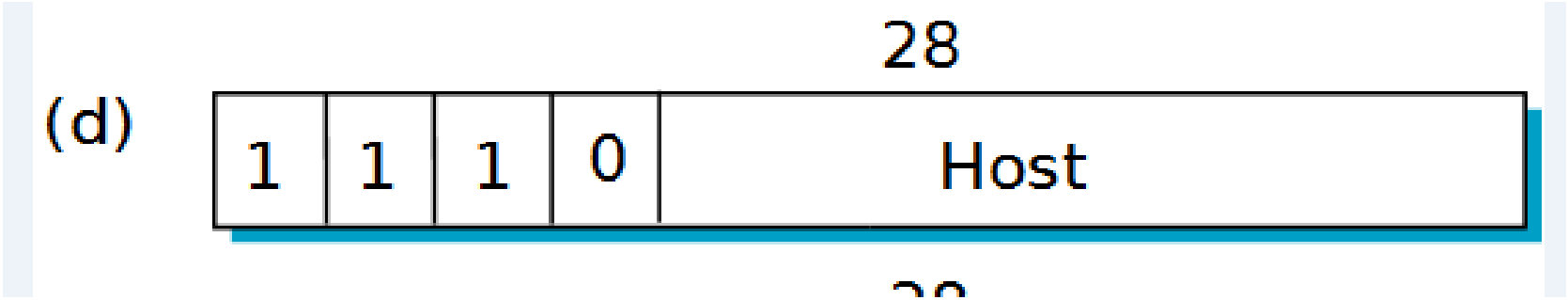
- This allows for 16,384 networks and 65,534 hosts per network.
- First byte of class B specifies decimal values from 128 to 191.
- Network block from 172.16.0.0 to 172.31.255.255 are reserved for Private addresses.
- The default subnet mask for Class B is 255.255.x.x.

- Class C
  - Class C addresses are used for small networks.
  - The three high-order bits in a class C address are always set to binary 1 1 0.
  - The next 21 bits (completing the first three octets) complete the network ID.
  - The remaining 8 bits (last octet) represent the host ID.
  - This allows for 2,097,152 networks and 254 hosts per network.



- The First Byte of class C specifies decimal value 192 to 223.
- Class C IP addresses range from 192.0.0.x to 223.255.255.x.
- The default subnet mask for Class C is 255.255.255.x.

- Class D
  - Class D addresses are reserved for IP multicast addresses.
  - The four high-order bits in a class D address are always set to binary 1 1 1 0.
  - The remaining bits are for the address that interested hosts recognize.
  - Microsoft supports class D addresses for applications to multicast data to multicast-capable hosts on an internetwork.



- The First Byte of class D specifies decimal value 224 to 239.
- Class D has IP address rage from 224.0.0.0 to 239.255.255.255.
- Class D does not have any subnet mask.

- Class E
  - Class E is an experimental address that is reserved for future use.
  - The high-order bits in a class E address are set to 1111.
  - First byte of the class E specifies decimal values from 240 to 255.

Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field		per network	Start address	End address
w‹	a		i‹	hilly	i6,n,»iy')aaei		ltziti‹l4
0st¿	II	II	1t	16,6(I!)	6,\$(t[1]')	UI(.I.I,I	1)1.III.II(.t6
mc	iia	i‹	i	i,a›7,iii\)	lx;/j	;isi.aaa	"uifiii‹›«
ID(JS);	111é	rilélel	) olMnd)	akind	r:tf drd	)Z4.g.0	'239.51.215.26
3aE(ist«dj	1111	nal6d	) olMnd)	dMld	nstédnd	j24é.0D,0	24.51.215.2S

Unicast IP Address

- Unicast IP Address means one to one communication.
- When data packet is sent from a host with destination address which represent a single host.
- This address belongs to class A, class B and clas C.

Multicast IP Address

- Multicast means one to many communications.
- When data packet is sent from a host to group of host.
- Multicast addresses belong to class D addresses.
- Multicast internet is of two types, local level and global level.

Broadcast IP Address

- Broadcast addressing means one to all communication.
- A broadcast address is an IP address that allows a data packet to be sent to all machines on a given network.
- Data packet is broadcast only on local level not on global level.

IP Subnet

- Sub netting means dividing a network further into several sub-networks where each sub-network has its own sub-network address.
- Instead of having a single huge network for an organization smaller networks within a given huge network are created.
- This is done with method called sub netting.
- In sub netting IPV 4 network is broken into two parts, Network Id and Host Id.

- Advantages of Subnet:
  - Single network is divided in to smaller network. Single network ID can be used by more than one network.
  - Size of Physical networks is reduced and hence easy to manage.
  - Physical damage to a network affects only a part of network.
  - Remote networks are employed by using a WAN link to connect local or remote local area network.

Subnet Mask

- Subnet mask specifies the part of IP address that is to be used for identifying a sub network.
- It is called a subnet mask because it is used to identify network address of an IP address by performing a bitwise AND operation on the net mask.
- A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address.

- Default Subnet mask:
  - 3 Classes are used for subnet Class A , Class B and Class C; each class has a default subnet mask.
  - Class A consist of eight 1s in the network address fields and twenty four 0s in remaining field.
  - Class B consist of sixteen 1s in the network address fields and sixteen 0s in remaining field.
  - Class C consist of Twenty-four 1s in the network address fields and eight 0s in remaining field.

Default Subnet Masks for Standard IP Address Classes

Class	Subnet Mask Bit Pattern	Subnet Mask
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

- The Number of 1s must match the number of network address bits and the number of 0s must match the number of host address bits.

Super netting

- A super network, or super net, is an Internet Protocol (IP) network that is formed from the combination of two or more networks (or subnets) with a common Classless Inter-Domain Routing (CIDR) prefix.
- Super netting, also called Classless Inter-Domain Routing (CIDR), is a way to aggregate multiple Internet addresses of the same class.
- The procedure used to create a super net is commonly called super netting.

- Super netting enables organizations to modify their network size and minimize the extensive requirement of network routing devices by combining several independent routes.
- Super netting simplifies network routing decisions and saves storage space on route tables.
- Super netting is most often used to combine Class C network addresses and is the basis for most routing protocols currently used on the Internet.

Special Addresses

- Special IP addresses are IP addresses which are never used on the public internet; which are used in private addresses, loop-back address and Link-Local addresses.
- The private addresses are used to communicate within a network which is not used in the public Internet.
- The loop-back address is used to test the network devices and working of network protocols.
- Link-local addresses which are used for IP address configuration in case of any of the IP address configuration protocols are unavailable.

IPV 6
(INTERNET PROTOCOL VERSION 6)

- IPV 6
  - Internet Protocol version 6 (IPv6) is the latest version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.
  - IPV6 is of 128 (16*8) bits represented in 8 combination of 4 hexadecimal numbers each, separated by colon.
  - IPV6 is called a 16-bit Hexadecimal colon delimited block.
  - Example:

    21DA**:**00D3**:**0000:2F3B:02AA:00FF:FE28:9C5A

- feature of IPV6
  - New header format
  - Large address space
  - Efficient addressing and routing infrastructure
  - Stateful address configuration
  - Built in security
  - New protocols for neighboring
  - Extensibility

Unicast IP address

- A unicast address identifies a single interface within the scope of the type of address.
- The scope of an address is the region of the IPv6 network over which the address is unique.
- Packet addressed to a unicast address are delivered to a single interface.

Multicast IP address

- With the appropriate multicast routing topology, packets addressed to a multicast address are delivered to all interfaces identified by the address.

Any cast IP address

- An Any cast addresses identifies multiple interfaces.
- With the appropriate unicast routing topology, packets addressed to an any cast address are delivered to a single interface- the nearest interface that is identified by the address.

IPV 4	IPv6
IPV 4 is developed in 1981.	IPV6 is developed in 1999.
IPv4 addresses are 32 bit length.	IPv6 addresses are 128 bit length.
IPv4 addresses are binary numbers represented in decimals.	IPv6 addresses are binary numbers represented in hexadecimals
IP Sec support is only optional.	Inbuilt IP Sec support.
Number of Address 2^32.	Number of Address 2^128.
Address Resolution Protocol (AR) is available to mapIPv4 address to MAC addresses.	Address Resolution Protocol (ARP) is replaced with a function of Neighbor Discovery Protocol (NDP).
Broadcast messages are available.	Broadcast messages are not available.

Steps of Migration From IPV4 to IPV6

1. Creating a report listing all of your current network infrastructure and their associated capabilities to supports IPv6.
2. Find out how your internet and WAN services provides will support IPV6.
3. Work with developers to evaluate your application portfolio for IPV 6.

4. Determine where to build an IPV6 network you may decide to deploy an IPV6 internal network.

- Tier transmission frame works for migration from IPv4 to IPv6.
- IPV6 supports mainly 3 types of migration methods from IPV4 to IPv6
  - Dual stack approach
  - Tunnel Approach
    - Static/manual
    - Automatic
  - Translation

Windows 2008 server

Introduction

- Windows server 2008 is an operating system that enables core IT resources, such as file and print sharing, remote access and security.
- It also provides a familiar windows user experience that helps you manage and safeguard business information.
- The basic terminology related to windows server 2008 are as follow.

1) Window Domain
   - A windows domain is a form of a computer network in which all user accounts, computers and other security principles, are registered with a central database (Called directory services) located on one or more central computers known as domain controllers.
   - Authentication take place on domain controllers.
2) Configuration
   - Computers can connect to a domain via LAN, WAN or using VPN connection.
   - Smart card and digital certificate can be used to confirm identities and protect stored information

3) Domain Controllers
   - A domain controller is a windows server that manages all security related aspects between user and domain interactions, centralizing security and administrators.
4) Active Directory
   - Computers inside an Active Directory domain can be assigned into organizational units according to location, organization structure or other factor.
5) Work Groups
   - Work Groups is the other model for grouping computers running windows in a networking environment.
   - Work group does not have server and client, that uses peer-to-peer networking.

Difference editions of Windows server 2008

1. Windows server 2008 standard:
   - It is standard edition of server 2008 and is directed to the SMB sector, the server with operating system will often play a role of domain controller, File and print server, DHCP server and application server.
   - These servers do not require more memory.
   - The 32 bit version supports up to 4GB RAM and up to 4 processor in SMP configuration
   - The 64 bit version supports 32 GB RAM and 4 processors SMP configuration.

2. Windows server 2008 Enterprise:
   - The enterprise edition will be intended for large companies running heavy application like SQL server or Exchange Server, these will be require ,ore memory than standard edition.
   - The 32 bit version supports up to 64 Gb of RAM and up to 8 processors in SMP configurations
   - The 64 bit version supports up to 2 TB of RAM and up to 8 processors SMP configurations.

3. Windows server 2008 Datacenter:
   - Data center Intended only to large enterprise marker, the main difference from the enterprise is on the number of virtual machines that can be uses with single license is unlimited.
   - License of the Datacenter will be associated with a physical server.
   - These servers typically cost tens or even hundreds of thousand of dollars.

4. Windows Web 2008:
   - This edition is indicated only for servers that run IIS services, the Microsoft web server.
   - The 32 bit supports up to 4 GB of RAM and 4 processors in SMP configuration.
   - The 64 bit supports up to 32 GB of RAM and 4 processors in SMP configuration.

5. Windows Server 2008 Server Core:
   - Windows server 2008 have two types, Full and server core installation.
   - Full installation is where most functions are managed via the GUI (Graphical /user Interface) of CLI (Command Line Interface).
   - Server core run only in CLI.

Installation of windows server 2008

- Hardware and software configuration:
  - Processor : Minimum 1 GHz (x84 processor) or 1.4GHZ (x64 processor)
  - Recommended 2 GHz or faster.

  - Memory: Minimum 512 MB RAM
  - Recommended 2 GB RAM or grater
  - Maximum (32-bit system) : 4 GB (Standard) or 64 Gb (Enterprise and Datacenter)
  - Maximum (64-bit system) : 32 GB (Standard) or 2 TB (enterprise and Datacenter)

- Available Disk: Minimum 10 GB
- Recommended 40 GB or Grater

- Drive : DVD-ROM drive

- Display and Peripherals: Super VGA (800 * 600(or higher resolution monitor
- Keyboard
- Mouse

Active Directory

- Active directory consist of logical and physical components.
- These components are used to develop directory structure for your organization.
- Domain, Organization Units, Tree and forest are components that represent the logical structure.
- Sites and domain controllers represents the physical structure.

Domain

- It stores the fundamental objects of a network.
- It is a central unit of a logical structure. The network objects such as the printers, documents, email addresses, databases and the users allows network community members to perform their respective task.
- The domain includes all network objects and their information.
- Network directory contains multiple domains.
- It includes the network objects and stores information of the objects.

Organization Units

- It allows you to administrator users and resources.
- The OU also contains objects such as user accounts, groups, computers, printers applications, file sharing.
- You can add OU to other OU to provide administrative control to it. This is called nesting.
- Controls user and computer accounts.

Tree

- Represents hierarchical arrangement of the windows server 2008 domains.
- To create hierarchy you must identify the parent child relationship among domains.
- Contains OUs, used to partition the directory data and controls
- Example : University.com

Forest

- It represent the hierarchical arrangement of the independent domain trees,
- All domain in the forest share the same schema and global catalog.
- Global analog is a central storage of the object information in the tree or forest residing on a domain controller.
- Contains domains used to defines the scope of authority of the administrators.

Event Logging

– Windows server includes two categories of event logs :Windows Logs and Applications and services Logs.

– You can either the event viewer or command line tool to manage event logs (Wevtutil).

1. Windows Log:
   - The windows logs category includes the logs that ware available on previous versions of the windows: the application, security and system logs.
   - Windows log are intended to store event from applications and events that apply to the entire system.

2. Application Log:
   - An Application logs contains events logged by applications or programs.
   - For example: The database program might record a file error in the application log.
3. Security Log:
   - The security log contains events such as valid and invalid logon attempts, as events related to resource use, such as cresting opening or deleting objects.

4. Set up Log:
   - Set up logs contains events related to application setup.
5. System Log:
   - The system log contains events logged by windows system components.
   - For example : failure of a driver or other system to load during startup
6. ForwardedEvents Log:
   - The forward events log is used to store events collected from remote computers.

MMC (Microsoft Management Control)

- MMC is a component in windows server 200 and above that provides system administrators and advanced users an interface for configuring and monitoring the system.
- The Microsoft Management Console (**MMC**) is an application that provides a graphical-user interface (GUI) and a programming framework in which consoles (collections of administrative tools) can be created, saved, and opened. ... **MMC** is considered to be a container for the actual operations, and is known as a "tools host."

UNIT-5

Basics of Network Security Internet Connection & Sharing

❖ Fundamental of Network Security

- Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, modification or accessible resources.
- Network security involves the authorization of access to data in a network, which controlled by the network administrator.
- User chooses or assigned an ID and Password or other authenticating information that allows them to access to information and programs within their authority.
- Network security secures the network as well as protecting and overseeing operations being done.
- There are basically 5 fundamentals of network security which are defined below.

1. **Keep Patches and Updates Current:**
   - Verify that office computers are running current versions of these much used programs:
   - Oracle, Java, Internet Explorer, Microsoft Office Suit, Adobe etc.
   - Make sure you keep an inventory to make sure all your devices are updated regularly.
2. **Use Strong Password:**
   - Your password should be comprised of at least 6 characters or more, and uses a combination of upper-case Lower-case Letters, number and symbols.
   - The SANS Institute also recommends that passwords be changed every few months at least, without duplication.
3. **Secure Your Internet and VPN (Virtual Private Network):**
   - You want the strongest possible protocols for encryption and authentication to protect your network/data from hackers while information is travelling over the internet.
   - Use cloud-based email and file sharing instead of a VPN
   - Create user-access policies.
   - Before granting mobile devices full access to the network, check them for up-to-date anti-virus, firewall and spam filters.
4. **Actively manage user access privileges:**
   - Managing employee access to critical data on an ongoing basis should not be overlooked. More than half of 5,500 companies recently surveyed by HP and the Ponemon Institute said that their employees had access to “sensitive, confidential data outside the scope of their job requirements.
   - When an employee’s job changes, make sure the IT department is notified so their access privileges can be modified to fit the duties of the new position.

5. **Clean up inactive accounts:**
   - Hackers use inactive accounts once assigned to contractors and former employees to gain access and disguise their activity.
   - Software is available for cleaning up interactive accounts over large networks with many users.

❖ Requirements of network security

1. **Identification:**
   - Determining the identity of the individual with whom you are communicating.
   - Identification is simply the process of identifying one's self to another entity.

2. **Authentication:**
   - Assurance of identity of person or originator of data
   - Authentication serves as proof that you are who you say or what you claim to be.
   - Authentication is required when communication over a network or logging onto a network.

3. **Access Control (Authorization):**
   - This refers to the ability to control the access in the network, how much information they can receive.
   - Unauthorized users are kept out
   - Access control is the determining of the level of authentication to a system, network, or information.

4. **Availability:**
   - This refers to whether the network, system, hardware, and software are reliable and can recover quickly and completely in the event of the interruption service.

5. **Confidentiality:**
   - Protection from disclosure to unauthorized persons
   - Also called privacy and by encrypting the information so that it is not meaning to unauthorized entities.

6. **Integrity:**
   - Maintaining data consistency
   - This refers to the ability to protect information data or transmission from uncontrolled, unauthorized entity.
   - Integrity can be used in reference to the proper functioning of a network, system, or application.

7. **Accountability:**
   - Ability to track what an individual or entity is doing on a network.
   - System maintains a record of function performed, files accessed and information altered by entity on the network.

8. **No-repudiation:**
   - The ability to prevent entities from denying (Refuse to give or grant) that information or files ware sent or received or that information or file were accessed or altered when in fact they ware.

❖ Policies, Standards, Procedures, baselines, guidelines

1. **Security Policy**
   - A security policy is a set of rules, practices, and procedures detecting how sensitive information is managed, protected and distributed.
   - A security policy is documents that express exactly what the security level, and it is written by higher management.
   - Policies are statements of higher management and goals
   - Acceptable use, internet access, logging, information security, etc.

2. **Standards**
   - Standards specify the use of specific technologies in a uniform manner
   - Operating systems, applications, server tools, router configurations, etc.
   - Standards vary by industry.
   - There are two standards in security information management – ISO 17799 and COBIT

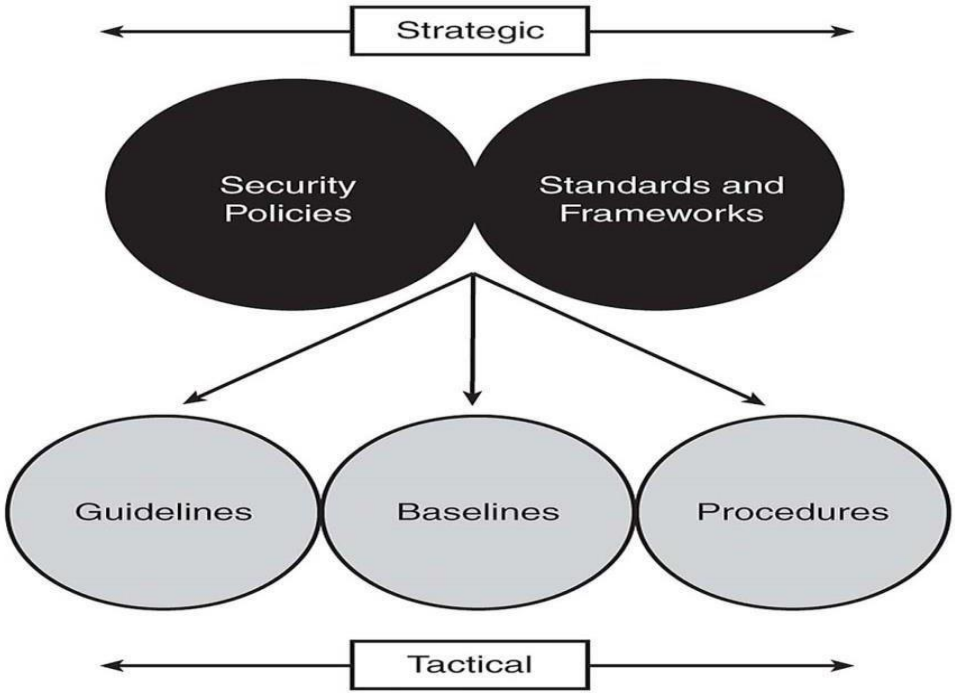


Fig-1 Strategic and Tactical Points of Network Security

3. **Procedures**
   - Procedures are detailed steps to perform a specific task
   - Procedures are low-level documents providing systematic instruction on how security policy and the standards are to be implemented in a system.
   - Adding user accounts, deleting user accounts, change management, etc.

4. **Baseline**
   - A Baseline is the minimum level of security requirement in a system.
   - Baselines are similar to standards but account for differences in technologies and versions from different vendors
   - Operating system security baselines
   - Mac OS X, Linux 5, Windows 2000, Windows XP, Windows Vista, Windows 7 etc.

5. **Guidelines**
   - Guidelines are recommended methods for performing a task by users.
   - Recommended, but not required.
   - A major difference between guidelines and standards is that guidelines can be used as reference, whereas standards are mandatory actions in most cases.

❖ Security methods

- There are mainly 3 types of security methods which prevents unauthorized users and unauthorized access of data in any network.
  - Encryption
  - Cryptography
  - Authentication

❖ Encryption

- Encryption is the conversion of electronic data into another form, called cipher text, which cannot be easily understood by anyone except authorized parties.
- The translation of data into a secret code.
- Unencrypted data is called plain text; encrypted data is referred to as cipher text.
- Following are key elements of security:
  - Authentication: the origin of a message can be verified.
  - Integrity: proof that the contents of a message have not been changed since it was sent.
  - Non-repudiation: the sender of a message cannot deny sending the message.

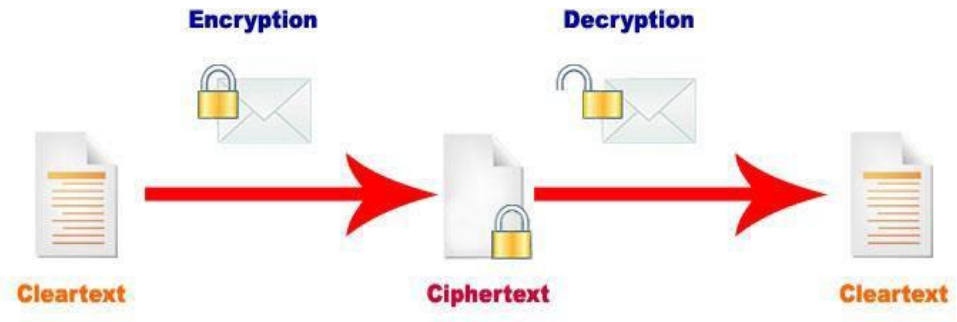


Fig-2: Encryption

- Decryption is the process of converting encrypted data back into its original form.
- Computer encryption systems generally belong in one of two categories:
  - Symmetric-key encryption
  - Asymmetric encryption / Public-key encryption

1. Symmetric-key Encryption

- Symmetric Encryption is an Encryption algorithm where the same key is used for both Encryption and Decryption.
- The key must be kept secret, and is shared by the message sender and receiver.

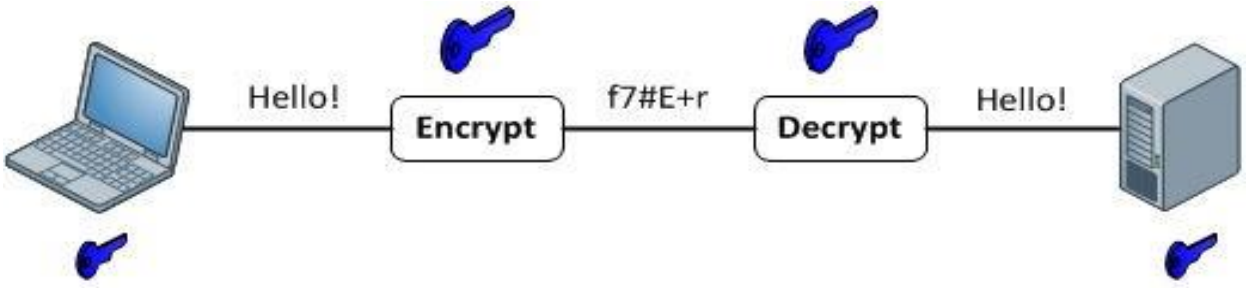


Fig-3 Symmetric-key Encryption

- Symmetric-key algorithms can be divided into two,
  - stream ciphers
  - block ciphers
- Stream Cipher
  - Stream ciphers encrypt the bits of the message one at a time
- Block Cipher
  - take a number of bits and encrypt them as a single unit
- Example of Symmetric Key Algorithms,
  - DES (Data Encryption Standards), 3DES, IDEA, RC4, Blowfish, CAST, AES (Advanced Encryption Standards)

A. DES (Data Encryption Standards):

- DES was developed by IBM in the mid-1970s.
- DES consists of algorithm and key.
- The key is a sequence of 8 bytes, each containing 8 bites for a 84-bit key.

- Each byte contains one parity bit, the key is actually 56 bits in length.
- DES is widely used in ATM (Automated Teller Machine) and Debit card system.

B. IDEA (International Data Encryption Algorithm):

- IDEA is symmetric key block cipher developed at the Swiss Federal Institute in 1990s.
- IDEA utilizes a 128 bit key.
- It is more efficient to implements in the software than DES.

C. RC4 (Rivest Cipher #4):

- Developed by Ron Rivest, it is stream Cipher that uses a variable size key.
- The approved expert version only used a 40 bit key.
- RC4 is used in Netscape Navigator and Internet Explorer.

D. CAST:

- The CAST was developed by Entrust Technologies, and It is available for free commercial and non-commercial use.
- The cast algorithm supports variable key lengths, anywhere from 40 bits to 256 bits in length.
- CAST is two to three time faster than DES and six to nine times faster than 3DES.
- Cast is employed in Pretty Good Privacy (PGP).

2. Asymmetric-key Encryption

- It is also known as Public-key Encryption.
- Asymmetric cryptography, requires two pair of separate keys, one is private key an is public key.
- The public key is used to encrypt plaintext or whereas the private key is used to decrypt cipher text.
- The public key is widely distributed, while the private key is known only to its proprietor.
- Example of asymmetric encryption,
  - DSA (Digital Signature Algorithm)
  - RSA (Rivest-Shamir-Adelman)

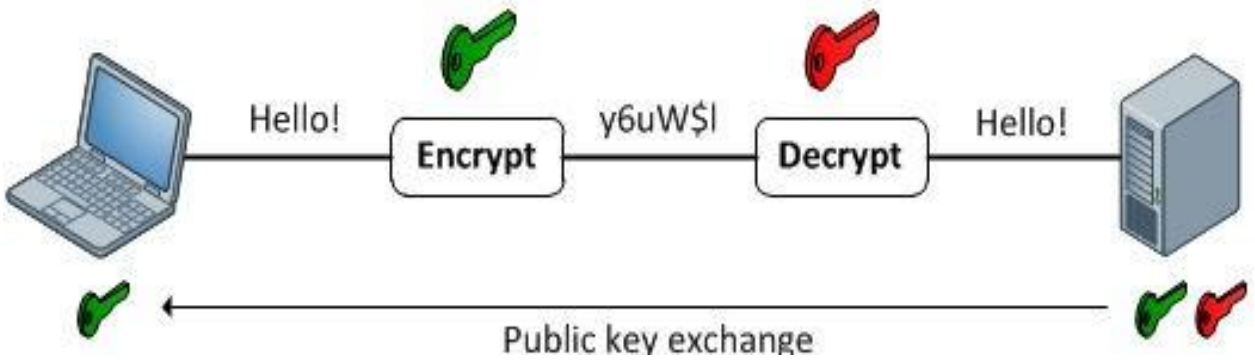


Fig-4 Asymmetric Key Encryption

A. Diffie-Hellman :

- The Diffie-Hellman algorithm was developed by Diffie and Martin Hellman at Stanford University.
- It was the first usable public key algorithm.

B. RSA (Rivest, Shamir, Adelman):

- The RSH was developed by Ron Rivest, Adi Shamir and Len Adelman at MIT.
- RSA multiplies large prime numbers together to generate keys.
- It is difficult to factor the product of large prime numbers.
- This algorithm is one of the most often associated with public key encryption.

C. DSA (Digital Signature Algorithm):

- DSA was developed as part of the Digital Signature Standards (DSS).
- DSA is not for encryption but for digital Signature.

D. MD 4 and 5 (Message Digest 4 and 5):

- MD 4 and 5 also created by Ron Rivest.
- MD 4 and 5 creates a unique 128 bit message digest value derived from the contents of a message or file.
- This value which is fingerprint of the message or file content is used to verify the integrity of the messages or file's contains.
- Id message or file is modified in any way, even a single bit, the MD5 cryptography checksum for the message or file will be different.
- MD5 is more secure than MD4.

3. Hash code Encryption

- Unlike secret key and public key algorithms, hash functions, also called message one-way encryption, have no key.
- Instead, a fixed-length hash value is computed based on the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered.
- The hash value provides a digital fingerprint of a message's contents, which ensures that the message has not been altered by an intruder, virus, or by other means.
- Hash code security implemented in email services.

❖ Authentication

- Authentication is a process that ensures and confirms a user's identity.
- A process in which user identified his/her self to the system.

- Assurance of identity of person or originator of data
- Authentication serves as proof that you are who you say or what you claim to be.
- Authentication is required when communication over a network or logging onto a network.
- Widows server 2003 provides a few different authentication types which can be used to verify the identities of network users,
  - NT LAN Manager (NTLM) authentication protocol
  - Secure Sockets Layer/ Transport Security Layer (SSL/TSL)
  - Smart Cards
  - VPN (Virtual Private Network) and RAS (Remote Access Service)
  - Kerberos authentication protocol
- SSL and TSL authentication is used for web application.
- Kerberos authentication protocol is the default authentication type for a windows server 2003 environment.
- Kerberos authentication protocol provides the following authentication features:
  - Verifies the identify of network users
  - Verifies whether the network services that a user is attempting to access is valid.

❖ Cryptography

- Information security uses cryptography to transform usable information into a form that renders it unusable by anyone than an authorized user, this process is called Encryption.
- Information that has been encrypted can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption.
- Cryptography is used in information security to protect information from unauthorized or accidental discloser while information is in transits (Electronically or physically) and while information is in storage.
- Cryptography provides Information security with other useful application as well including authentication methods, message digest, digital signatures, non-repudiation an encrypted network etc.
- Software application such as GNUPG and PGP can be used to encrypt data files and Email.
- Cryptography can introduce security problems when it is not implemented correctly.
- Wireless communications can encrypt using the WAP or WEP Protocols.

1. Private key Cryptography

- Also known as symmetric cryptography.
- It is simple in nature because the secrete key that is used for both encryption and decryption is shared between the sender and receiver.
- Before the communication can occur the sender and receiver must exchange a shared secrete key.
- The encryption key and its matching decryption key are often referred to as a public/private key pair.
- Some of the common algorithms like DES, AES etc., are used.
- The private key of the recipient is used to decrypt message, and only the recipient must be able to access it.

- It is difficult to deliver the private key.
- It requires as many key as number of recipients.

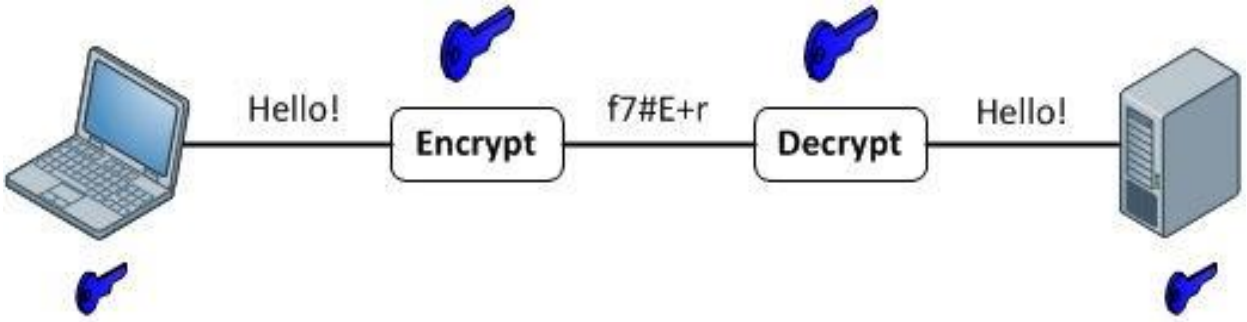


Fig-5 Private Key Cryptography

- Advantages:
  - Fast
  - Relatively Secure
  - Widely Understood
- Disadvantages:
  - Required secrete sharing
  - No authentication
  - No non repudiation

2. Public key Cryptography

- The most common Algorithm of asymmetric algorithm is MD5, RSA, and DSA.
- Asymmetric encryption requires more processing resources than symmetric encryption.
- In public key encryption there are two key one is public and second is private.
- Encrypted texts by public key can be decrypted by the private key.
- One public key can enough for any number of receivers.
- Key deactivations techniques are often used to add variability to share secretes that are used over multiple message exchanges.

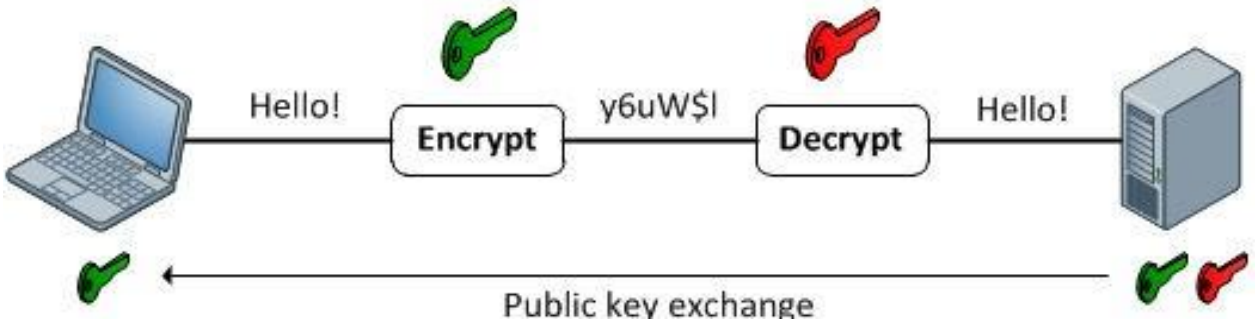


Fig-7 Public Key Cryptography

- Advantages:

- No secrete sharing necessary
- Provides non repudiation

- Disadvantages:
  - Slower intensive
  - Certificate authority required

❖ CIA Model (Confidentiality, Integrity, Availability)

- A simple and widely used security model is the CIA .
- These three (Confidentiality, Integrity, Availability) key principals should guide all secure system.
- CIA provides the measurement tool for security implementation.
- These principles are applicable across the entire spectrum of security analysis- from access, to a user internet history, to the security of encrypted data across internet.

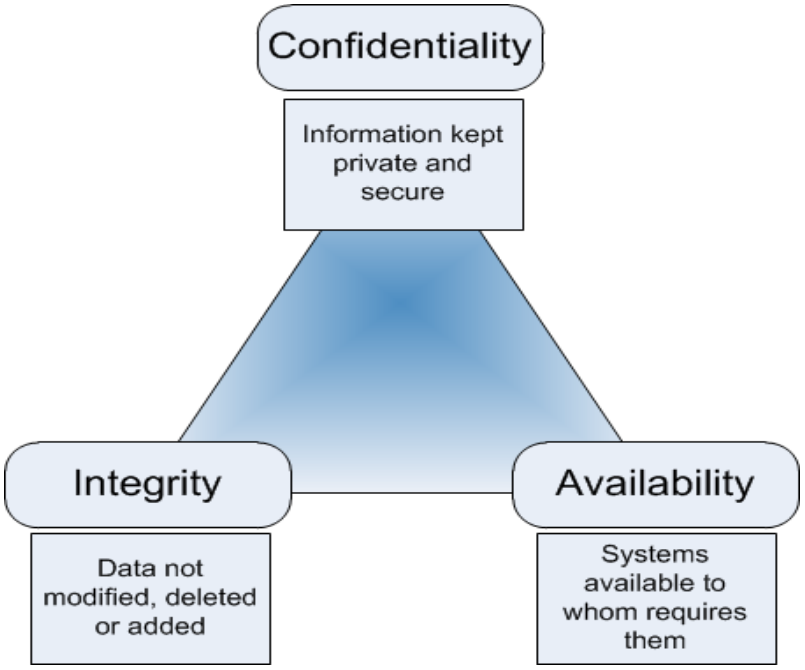


Fig-6 CIA Security Model

1. Confidentiality

- Confidentiality is the ability to hide information from those people unauthorized to view it.
- Authentication methods like user-IDs and passwords, that uniquely identify data systems, users and control access to data systems and resources is the goal of confidentiality.
- Protection from disclosure to unauthorized persons.
- Also called privacy and by encrypting the information so that it is not meaning to unauthorized entities.

2. Integrity

- Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle.
- Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people.
- Integrity prevents unauthorized modification of data, systems and information, thereby providing accordance of the information systems.
- A common type of security attack is man-in-middle.
- In this type of attack, an intruder intercepts data in transfer and makes changes to it.

3. Availability

- Availability refers to the availability of information resources.
- Availability is the prevention of the loss of access to resources and information to ensure that information is available for use when it is needed.
- Systems, access channels, and authentication mechanisms must all be working properly for the information they provide and protect to be available when needed.

Internet Connection and Sharing

❖ What is Internet?

- The Internet began in 1969 as the U.S. Department of Defense's Advanced Research Project Agency (ARPA) to provide immediate communication within the Department in case of war.
- The project was called ARPA net and it is the foundation of the internet.
- The Internet is not owned or operated by any one entity.
- This worldwide computer network allows people to communicate and exchange information in new way.
- The internet is the largest computer network in the world, connection millions of computers.
- A network is a group of two or more computer system linked together.
- The internet is a worldwide telecommunications system that provides connectivity for millions of other, smaller networks; therefore, the Internet is often referred to as a network of networks.
- The Internet acts as a pipeline to transport electronic messages from one network to another network. At the heart of most networks is a server, a fast computer with large amounts of memory and storage space.
- An Internet Service Provider (ISP) allows the user access to the Internet through their server.
- You can connect to the Internet through telephone lines, cable modems, cell phones and other mobile devices.

❖ What makes up the World Wide Web?

- The Internet is the collection of the many different systems and protocols.
- The World Wide Web, developed in 1989, is actually one of those different protocols.
- The World Wide Web contains a vast collection of linked multimedia pages that is ever-changing.
- There are several basic components of the Web that allow users to communicate with each other.

- TCP/IP Protocols:
  - In order for a computer to communicate on the Internet, a set of rules or protocols computers must follow to exchange messages was developed.
  - The two most important protocols allowing computers to transmit data on the Internet are Transmission Control Protocol (TCP) and Internet Protocol (IP).
  - For instance, if a user is running Windows on a PC, he or she can communicate with iPhones

- Domain name system:
  - An Internet address has four fields with numbers that are separated by periods or dots.
  - This type of address is known as an IP address.
  - Rather than have the user remember long strings of numbers, the Domain Name System (DNS) was developed to translate the numerical addresses into words. For example, the address www.saurastrauniversity.edu is really 131.247.120.10.

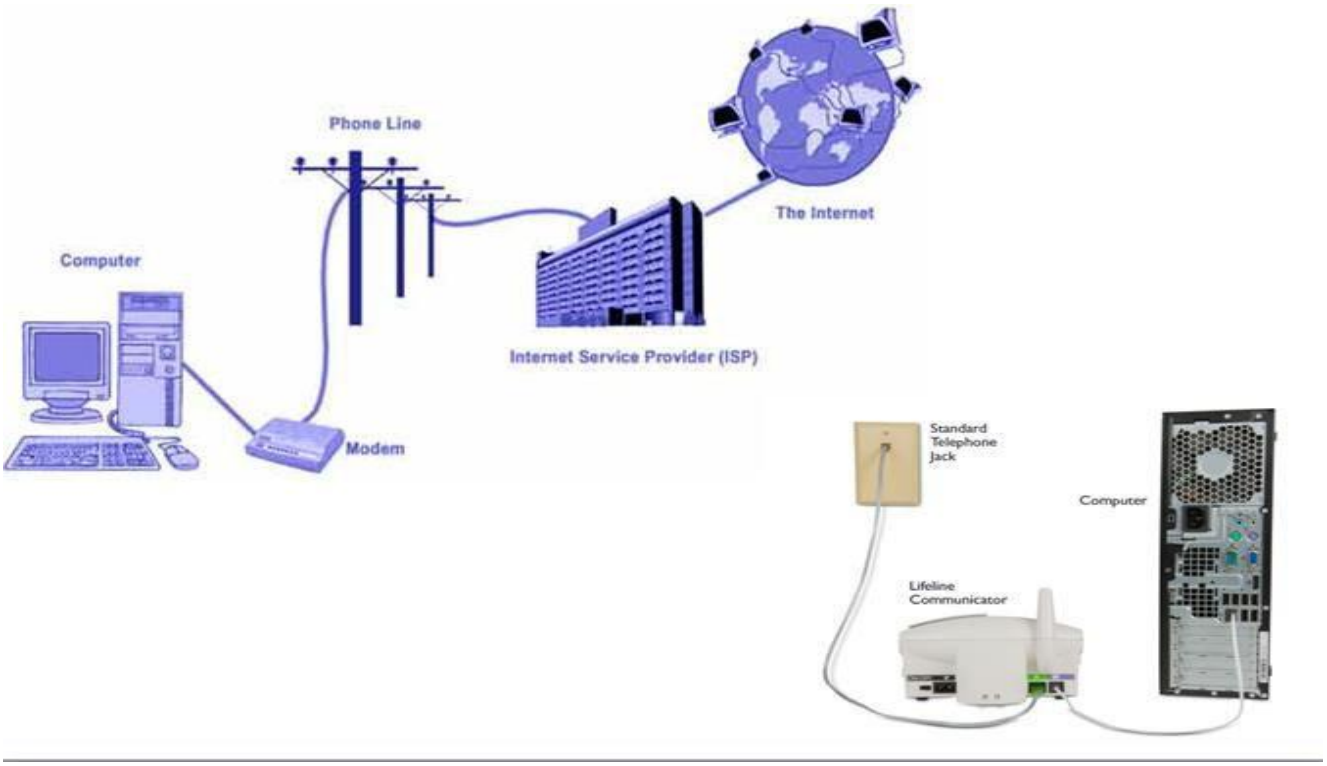
- URL (Uniform Resource Locator) :
  - Addresses for web sites are called URLs (Uniform Resource Locators). Most of them begin with http (Hyper Text Transfer Protocol), followed by a colon and two slashes.
  - For example, the URL for the Florida Center for Instructional Technology is http://saurastrauniversity.edu/

- Top-level domain:
  - Each part of a domain name contains certain information. The first field is the host name, identifying a single computer or organization. The last field is the top-level domain, describing the type of organization and occasionally country of origin associated with the address.
  - Top-level domain names include:
    - .com Commercial
    - .edu Educational
    - .gov Government
    - .mil Military
    - .org Non-profit Organization
  - Domain name country codes include, but are not limited to:
    - .au Australia
    - .de Germany
    - .fr France
    - .in India
    - .uk United Kingdom
    - .us United States

❖ Technology Related Internet

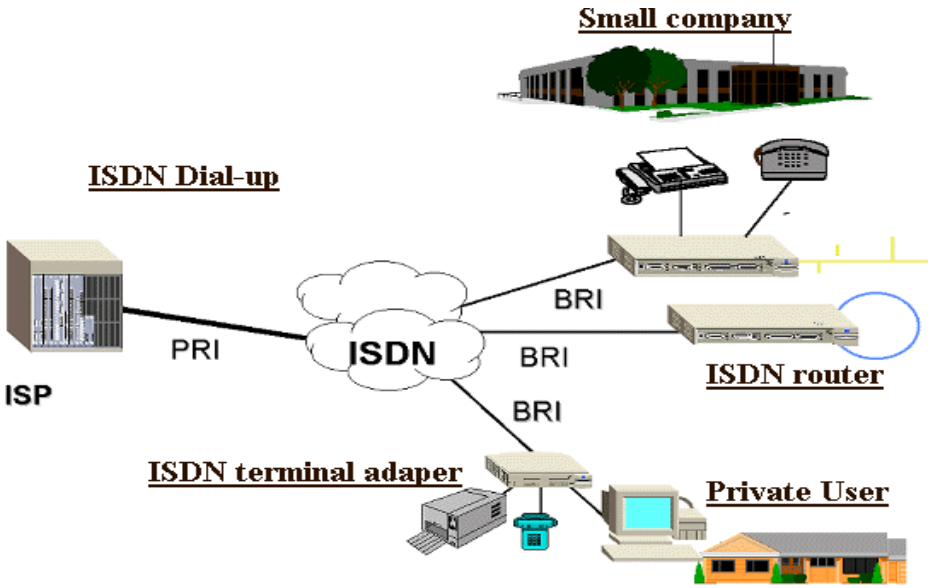
1. Dial up Technology

- 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 computers 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 dialed connection to an ISP via telephone lines.
- The user's computer or router uses an attached modem to encode and decode Internet Protocol packets and control information.
- Dial up connection to the internet require no Infrastructure other than the telephone network.
- Dial up often the only choice available for ruler or remote areas, where broadband installations are not possible.
- Dial up access is temporary connection, because either the user, ISP or phone company terminates the connections.
- Dial up requires time to establish a telephone connection and perform handshaking for protocol synchronization before data transfers can take place.
- A 2008 Pew Internet and American Life Project study states that only 10 percent of the US people still used dial up internet access.



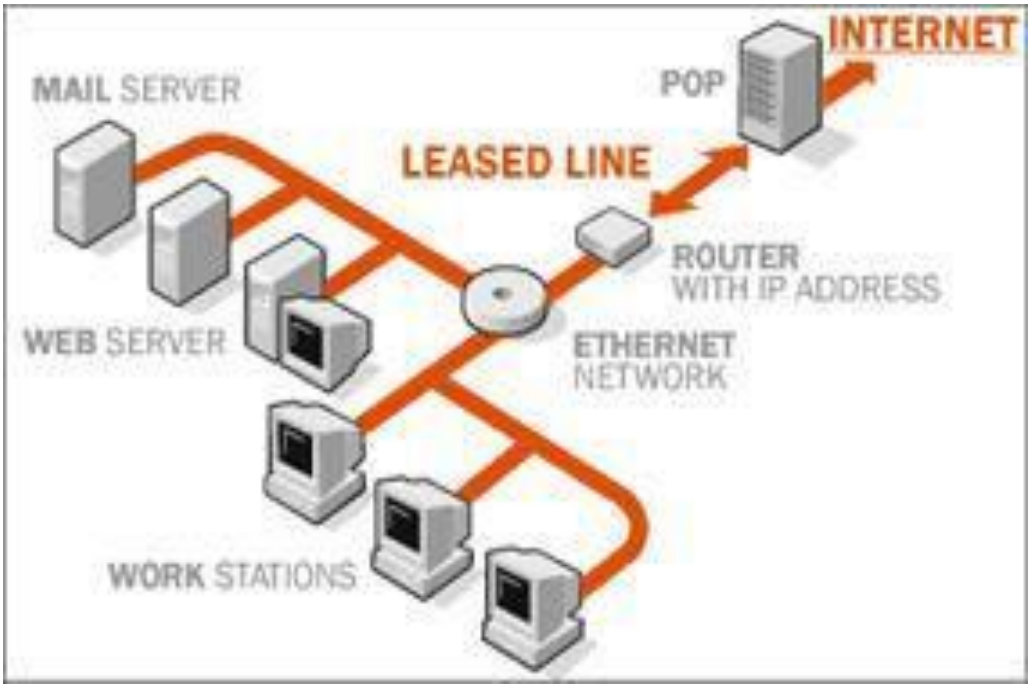
2. ISDN Technology

- ISDN stands for Integrated Services Digital Network.
- Integrated Services for Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network.
- ISDN provides a standard interface for voice, fax video, graphics and data – all on a single telephone line.
- ISDN requires adapters at both ends of the transmission so your access provider also needs an ISDN adapter.
- ISDN Internet service generally supports data rates of 128 Kbps.
- There are several kinds of access interfaces to ISDN defined as Basic Rate Interface (BRI), Primary Rate Interface (PRI), Narrowband ISDN (N-ISDN), and Broadband ISDN (B-ISDN).
- BRI intended for the home and small enterprise and PRI for longer users.
- BRI and PRI include a number of B-channels and D-channels.
- Bearer Channels: B- Channel carries data, voice and other services.
- Signaling Channel: D-channel carries control and signaling information.
- In a videoconference, ISDN provides simultaneous voice, video and text transmission between individual desktop videoconferencing system and group conferencing system.
- In INDIA BSNL and Airtel are largest communication service providers and offer both ISDN BRI and PRI service across the country.



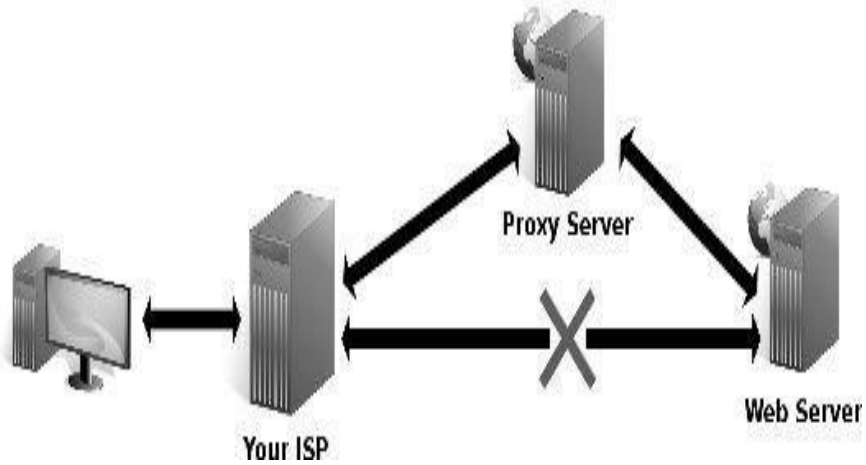
3. Leased Line Technology

- Leased line is a service contract between a provider and a customer, whereby the provider agrees to deliver a telecommunications line connecting two or more locations in exchange for a monthly rent.
- Leased lines can be used for telephone, data or Internet services.
- An Internet leased line is a premium internet connectivity product, delivered over fiber normally, which is dedicated and provides uncontended, 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.
- In India, leased lines are available at speeds of 64 kbps, 128 kbps, 256 kbps, 512 kbps, 1 Mbps, 2 Mbps, 4 Mbps, 8 Mbps, 16 Mbps T1(1.544 Mbps) or E1(2.048 Mbps).
- Customers are connected either through telephone lines, ADSL, or through Wi-Fi.
- Leased lines are used to build private network, private telephone networks re access the internet or extranet.
- Leased line services become digital in the 1970s with the conversion of the Bell backbone network from analog to digital circuits.
- Leased line ware used to connect mainframe computers with terminals and remote sites, via IBM system architecture or DECnet.
- Leased lines are more expensive than alternative connectivity services including (ADSL, SDSL, etc) because they are reserved exclusively to the leaseholder.



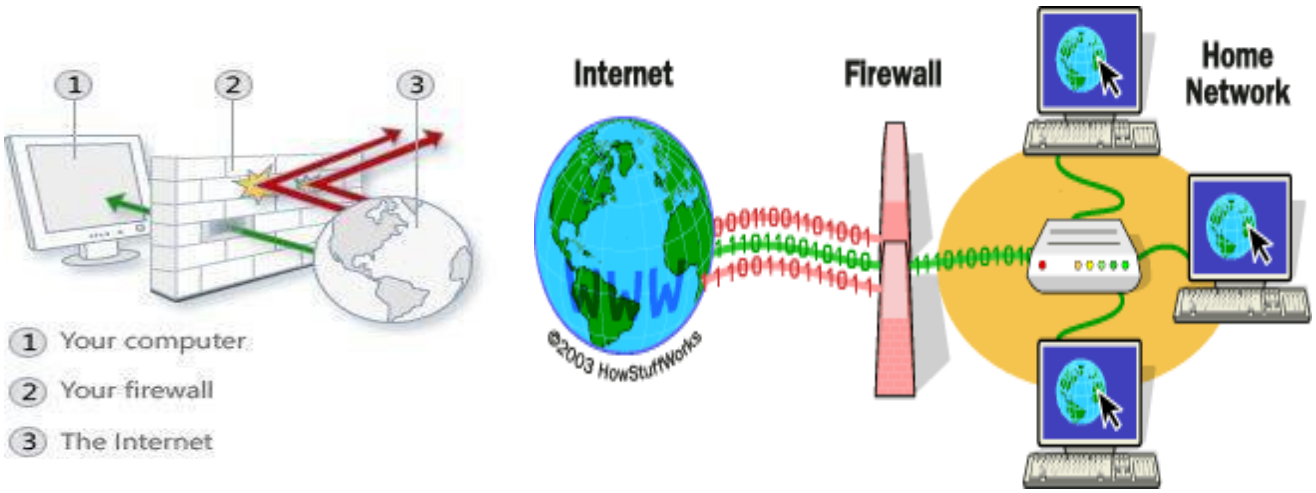
❖ Proxy Server

- A proxy server is computer that functions as an intermediary between a web browser (such as Internet Explorer) and the Internet.
- Proxy servers help improve web performance by storing a copy of frequently used webpages.
- When a browser requests a webpage stored in the proxy server's collection (its cache), it is provided by the proxy server, which is faster than going to the web.
- Proxy servers are used mostly by networks in organizations and companies. Typically, people connecting to the Internet from home will not use a proxy server.
- An anonymous proxy server acts as a middle man between your browser and an end server.
- Instead of connecting the end server directly to get a web page, the browser connects the proxy server, which forwards the request on the end server.
- No direct connection between the client and the destination server.



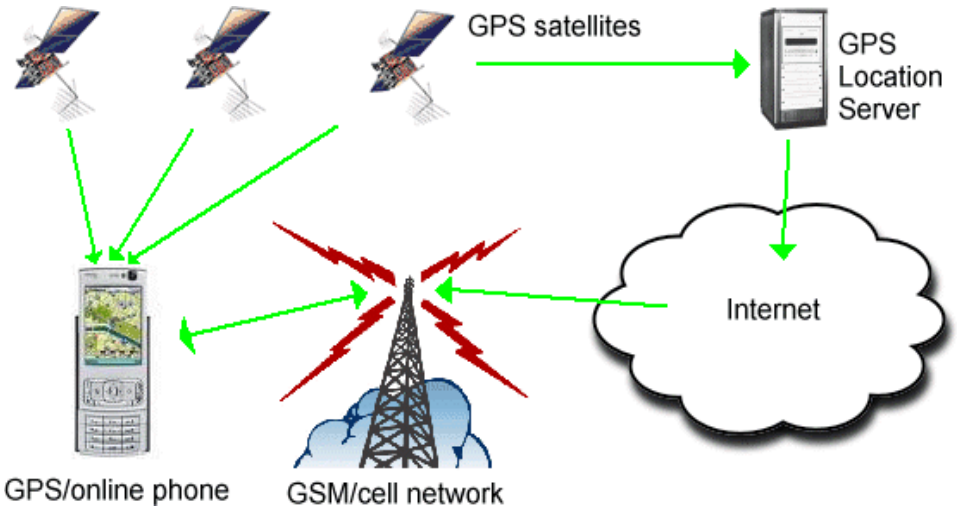
❖ Firewall

- A firewall is a network security system, either hardware or software based, that controls incoming and outgoing network traffic based on a set of rules.
- 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.
- A firewall has a set of rules which are applied to each packet.
- The rules decide if a packet can pass, or whether it is discarded.
- 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 ended in April 2014.



❖ GPS (Global Positioning System)

- GPS was developed by the United States Department of Defense.
- It uses between 24 medium Orbit Satellites that transmit Microwave signals.
- This enables GPS receivers to determine their current location and time.
- The GPS satellites are maintained by the United State Air Force.
- The Global Positioning System (GPS) is a satellite-based navigation system made up of a network of 24 satellites placed into orbit by the U.S. Department of Defense.
- GPS was originally intended for military applications, but in the 1980s, the government made the system available for civilian use.
- GPS works in any weather conditions, anywhere in the world, 24 hours a day. There are no subscription fees or setup charges to use GPS.
- GPS used by civilians as a navigation system.
- The result is provided in the form of a geographic position longitude and latitude – to, for most receiver with in an accuracy of 10 to 100 meters.
- Application of GPS:
    - Aviation (Aircraft) ,Marin , Rail , Space, Agriculture, Surveying and Mapping, Road and Highways etc.



❖ GPRS (General packet radio service)

- GPRS is a type of wireless data connection. It stands for General Packet Radio Service.
- GPRS is a packet oriented mobile data service available to users of the 2G and 3G cellular communication systems, Global System for Mobile communication (GSM) and Time Division Multiple System (TDMA).
- GPRS was originally standard by European Telecommunications Standard Institute (ETSI).
- In 2G General Packet Radio Services (GPRS) provide data rates from 56 up to 114 Kbps and continuous connection to the Internet for mobile phone and computer users.
- In 3G GPRS can reach speeds between 120Kbps to 384Kbps.
- GPRS usages typically charged based on volume of data transferred, contrasting with circuit switched data, which is usually billed as per minute of connection time.
    - Services Offered by GPRS
    - SMS massaging
    - "Always on" Internet access
    - MMS (Multimedia Messaging Service)
    - Internet Application for Smart devices through Wireless Application Protocol (WAP).
- GPRS divided into 3 classes based on hardware.
- Class A: Class A terminals can handle packet data and voice at the same time.
- Class B: Class B terminals can handle both packet data and voice, but not at the same time. Means during GSM (Voice call or SMS), GPRS services is suspended and resumed automatically after GSM service has concluded.
- Class C: Are connected to either GPRS services or GSM service (Voice call or SMS). Must be switch manually between one or the other services.

❖ CCTV (Closed Circuit Television)

- Closed-circuit television (CCTV), also known as video surveillance, is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors.
- CCTV relies on strategic placement of cameras and private observation of the camera's input on monitors.

- The system is called "closed-circuit" because the cameras, monitors and/or video recorders communicate across a proprietary coaxial cable run or wireless communication link.
- Term is most often applied to those used for surveillance and security in areas that may need monitoring such as banks, casinos, airports, military installations, and convenience stores.
- A more advanced form of CCTV, utilizing digital video recorders (DVRs), provides recording for possibly many years, with a variety of quality and performance options.
- IP CCTV cameras stream live video via digital packets across an internet protocol network such as LAN or the Internet.
- This means that video access remotely via a smart phone, Tablets or other network devices, and can be stored remotely.
- HD-Serial Digital Interface (SDI) came from the SDI broadcast standard developed by SMPTE for transmitting video.
- HD-SDO is used for transmission high definition video images (1280*720p or 1920*1080p) over existing analog infrastructure, or high end coaxial cables.
- The Price of CCTV camera based on Its Standard (HD or Normal camera) and Storage Capacity.

❖ VPN (Virtual Private Network)

- A Virtual Private Network (VPN) is a network technology that creates a secure network connection over a public telecommunication infrastructure such as the Internet or a private network owned by a service provider.
- The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.
- A VPN (Virtual Private Network) is a way of creating a secure connection 'to' and 'from' a network or a computer.
- The VPN uses strong encryption and restricted, private data access which keeps the data secure from the other users.

❖ Types of VPN

1. Site-to-Site VPN (Intranet based and /Extranet based):

- Site-to-site VPNs connect entire networks to each other; this means, site-to-site VPN can be used to connect a branch or remote office network to a company headquarters network.
- Each site is equipped with a VPN gateway, such as a router, firewall, VPN concentrator, or security appliance.
- There are two types of S2S VPN,
    - Policy Based
    - Routed

2. DMVPN: Dynamic Multipoint Virtual Private Network

- DM VPN is a dynamic tunneling form of a virtual private network (VPN) supported on Cisco IOS-based routers and Unix-like Operating Systems based on the standard protocols, GRE and IPsec.

- This DMVPN provides the capability for creating a dynamic-mesh VPN network without having to pre-configure (static) all possible tunnel end-point peers, including IPsec (Internet Protocol Security) and ISAKMP (Internet Security Association and Key Management Protocol) peers.

❖ VPN Protocols:

- VPN requires 3 protocols,
  PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), IP Sec (Internet Protocol Security)

1. PPTP (point-to-point tunneling protocol)

- This is the most common and widely used VPN protocol.
- They enable authorized remote users to connect to the VPN network using their existing Internet connection and then log on to the VPN using password authentication.
- They don't need extra hardware and the features are often available as inexpensive add-on software.
- The disadvantage of PPTP is that it does not provide encryption and it relies on the PPP (Point-to-Point Protocol) to implement security measures.
- PPTP is the first VPN protocol that was supported by Microsoft Dial-up networking.
- A specification of PPTP was published in July 1999 as RFC 2637.
- OS X and iOS are bundled with a PPTP client.
- Many different mobile phones with android as the operating system support PPTP as well.

2. L2TP I(Layer 2 tunneling protocol)

- L2TP or Layer to Tunneling Protocol is similar to PPTP, since it also doesn't provide encryption and it relies on PPP protocol to do this.
- The difference between PPTP and L2TP is that the data provides not only data confidentiality but also data integrity.
- L2TP was developed by Microsoft and Cisco.
- L2TP allows multiprotocol traffic to be encrypted and then sent over any medium that supports point to point datagram, such as IP or ATM.
- L2TP published in 1999 as proposed standard RFC 2661.
- L2TP is often used by ISPs when internet service over.
- L2TP is installed with the TCP/IP protocol.

3. IP Sec (Internet Protocol Security)

- IP sec is a protocol suite for securing Internet Protocol communications by authenticating and encrypting each IP packet of a communication session.
- IP sec can be used in protecting data flows (Traffics) between a pair of host-to-host (Hosts), between pair of network-to-network (Gateways) or between network-to-host (Network and Host).
- IP sec is an end to end security scheme operating in the Internet layer of the Internet Protocol Suite.

Full Form

- ARPA : Advanced Research Project Agency
- URL : Uniform Resource Locator
- ISP :Internet Service Provider
- ISDN : Integrated Services Digital Network
- VPN : Virtual Private Network
- GPS : Global Positioning System
- GPRS : General Packet Radio Service
- CCTV : Closed-circuit television
- L2TP : Layer 2 Tunneling Protocol
- PPTP : point-to-point tunneling protocol
- IP Sec : Internet Protocol Security
- ISAKMP : Internet Security Association and Key Management Protocol
- DMVPN: Dynamic Multipoint Virtual Private Network
- SDI : Serial Digital Interface
- BRI : Basic Rate Interface
- PRI: Primary Rate Interface
- N-ISDN ; : Narrowband Integrated Services Digital Network
- B-ISDN Broadband Integrated Services Digital Network
- GSM : Global System for Mobile communication
- PSTN : Public Switched Telephone Network